

# Exhibit **1** : Version 2.9

**Texas Department of Information Resources**

**Data Center Services Request for Offer**

**Public Cloud Manager**

**Statement of Work (SOW)**

## Table of Contents

<b>Contract Change Log</b>	<b>4</b>
<b>1. Business Background and Objectives</b>	<b>27</b>
1.1. Background Overview	27
1.2. Multi-sourcing Service Integrator (MSI)	27
1.3. PCM Scope and Eligible Customers	28
1.4. Service Objectives	28
<b>2. Transition Services</b>	<b>30</b>
2.1. Operations Take Over	30
2.2. General Transition Requirements	30
2.3. Knowledge Transfer	31
2.4. Transition Management Requirements	31
2.5. Transition Project Plan	32
<b>3. Steady State Operations and Support Services</b>	<b>39</b>
3.1. General Requirements	39
3.2. DCS Public Cloud Center of Excellence (CoE)	41
3.3. Procurement Management	44
3.4. Operations and Monitoring	45
3.5. Production Control and Scheduling	46
3.6. Technical Services	47
3.7. Network Services	52
3.8. Storage Services	53
3.9. Backup and Recovery Services	54
3.10. Middleware Services	57
3.11. Database Management Services	58
3.12. Disaster Recovery Services	61
3.13. Cloud Provider Sourcing Support Requirements	65
3.14. Critical Support Services	68
3.15. DIR Requested Projects	76
3.16. Reporting	78
3.17. Quality Assurance	79
3.18. Industry Standards, Certifications and Compliance	80
3.19. Obligation to Evolve	82
3.20. Operating Agreements with Other SCPs and MSI	83
3.21. Successful Respondent Cooperation	85
3.22. Onboarding New Customers	85
3.23. Project Bench	86
3.24. Enterprise SaaS Services	88
<b>4. Steady State Service Evolution and Optimization Services</b>	<b>88</b>
4.1. Environment Review and Advisory Services	88
4.2. Service Capacity Planning	89
4.3. Technology Planning and Optimization Roadmap	89
4.4. Annual Review of Service Roadmap	94
4.5. Public Cloud and Computing Optimization Services	95
<b>5. Successful Respondent Personnel Requirements</b>	<b>98</b>
5.1. Key Personnel Staffing	98
5.2. Key Service Personnel Positions	100
5.3. Staffing Requirements	101
5.4. Replacement, Qualifications, and Retention of Successful Respondent Personnel	103
5.5. Location of Services	105
5.6. Work Location(s) and Successful Respondent Personnel Involvement	105
5.7. Evergreen Service Personnel	106
5.8. Key Service Personnel	107
5.9. Personnel Experience, Accreditation and Certification Requirements	109
5.10. Transition Staffing Requirements	109
<b>6. Performance Model and Service Level Agreements</b>	<b>109</b>
6.1. General	109
6.2. Service Level Credits	111
6.3. Shared and Related Service Levels and Types	111
6.4. Reporting	111
6.5. Service Level Default	112

6.6.	Earnback.....	113
6.7.	Additions, Modification, and Deletions of Service Levels.....	114
6.8.	Service Delivery Failure: Corrective Action Plan.....	115
6.9.	Service Level Improvement Plans.....	116
6.10.	Service Level Escalation Event.....	117
6.11.	Service Level Definitions.....	117
6.12.	Recurring Critical Deliverables.....	117
6.13.	One-Time Critical Deliverables – After Effective Date.....	118
6.14.	Data Collection and Measuring Tools.....	118
6.15.	Percentage Objectives.....	119
6.16.	Low Volume.....	119
6.17.	Service Level Review.....	120
6.18.	Key Performance Indicators.....	121
6.19.	Operating Measurements.....	121
6.20.	Operational Reports.....	121
6.21.	Single Incident/Multiple Defaults.....	122
6.22.	Exceptions.....	122
6.23.	Exclusions.....	122
<b>7.</b>	<b>Transformation Projects.....</b>	<b>122</b>
7.1.	Transformation Principles.....	122
7.2.	Organization and Relationships of Transformation Projects.....	124
7.3.	Transformation Projects: Methodology.....	125
7.4.	DCS Customer Managed Public Cloud Instances.....	133
7.5.	Project Completion Activities, Final Documentation and Post Implementation Support Obligations.....	139
<b>8.</b>	<b>DCS Governance Model.....</b>	<b>139</b>
8.1.	Introduction.....	139
8.2.	Governance: Meetings.....	140
8.3.	Issue Management.....	142
<b>9.</b>	<b>Cross-Functional Services.....</b>	<b>144</b>
9.1.	General Operating Model Requirements.....	144
9.2.	Multi-sourcing Services Integration and Cooperation.....	144
9.3.	Shared Technology Services Documentation – Service Management Manual.....	144
9.4.	Marketplace and Portal Requirements.....	145
9.5.	MSI Tools and Operating Environment.....	146
9.6.	Service Catalog Management.....	147
9.7.	Outreach and Growth Requirements.....	147
9.8.	Customer Satisfaction Surveys.....	148
9.9.	Service Management Requirements.....	148
9.10.	Business Management.....	167
<b>10.</b>	<b>Contract Management.....</b>	<b>170</b>
10.1.	Contract Changes.....	170
10.2.	Deliverables.....	170
10.3.	Deliverable Acceptance Criteria.....	170
10.4.	Deliverable Expectation Document (DED).....	171
10.5.	Deliverables Review Meeting.....	172
10.6.	Acceptance Review Period.....	172
10.7.	Noncompliance.....	173
10.8.	Failure to Cure a Noncompliance.....	173
10.9.	Remediation of Defects in Previously Accepted Items.....	174
10.10.	Deliverables Credits.....	174
<b>11.</b>	<b>Contract Conclusion Requirements: Transition to Successor at Contract Termination.....</b>	<b>175</b>
11.1.	Overview.....	175
11.2.	Termination Assistance Services.....	175
11.3.	Successful Respondent Sourced and Managed Contracts.....	183
11.4.	Termination Assistance Plan.....	183
11.5.	Termination Management Team.....	184
11.6.	Operational Transfer.....	184
<b>12.</b>	<b>Other Requirements.....</b>	<b>185</b>
12.1.	Support Requirements.....	185
12.2.	Materials.....	185

### Contract Change Log

Amendment/CCR #	Date	Description of Changes
First Amendment/ CCR-000404	7/6/2020	<ul style="list-style-type: none"><li>• Modifies Section 3 Steady State Operations and Support Services to clarify and add requirements related to procurement, contract and operational services the Service Provider will provide as the contract holder</li></ul>
CCR-000427	09/29/2020	<ul style="list-style-type: none"><li>• Modifies 1.4.1 (a) (iii) to remove language requiring DIR approval of Sandbox support</li></ul>

## **TABLE OF DOCUMENTS:**

### **RFO**

Attachment 1: Respondent Information Form

Attachment 2: HUB Subcontracting Plan

Attachment 3: Respondent Release of Liability

### **Master Services Agreement (MSA)**

Attachment 1: Form of Nondisclosure

Attachment 2: Insurance and Risk of Loss

Attachment 3: Form of Source Code Escrow (if applicable)

Attachment 4: Form of Parent Guaranty

### **Exhibit 1 Public Cloud Manager Statement of Work (Exhibit 1 SOW) (this document)**

#### **Attachments**

Attachment 1.1: Deliverables

Attachment 1.2: Service Level Matrix

Attachment 1.3: Service Level Definitions and Performance Analytics

Attachment 1.4: SMM Content and Organization

Attachment 1.5: Key Personnel

#### **Appendices**

Appendix A – Reports

### **Exhibit 2 Public Cloud Manager Provisions and Pricing (Exhibit 2 Pricing)**

Attachment 2.1: Pricing and Volumes

Attachment 2.2: Financial Responsibility Matrix

**Table 1 Terms and Definitions**

Term	Definition
Acceptance or Accepted	The determination, in the Department of Information Resources (DIR) or, if applicable, DCS Customers' reasonable discretion and in accordance with the relevant provisions of Article <a href="#">10 Contract Management</a> , confirmed in writing by DIR or the applicable DCS Customer, that Software, Equipment, Systems, and/or other Deliverables are in Compliance, in accordance with <b>Master Services Agreement (MSA) Section 8.4.3 Developed Materials Compliance</b> and the Services Management Manual (SMM) or other criteria agreed to in writing by the Parties.
Acceptance Criteria	The criteria that Successful Respondent must confirm have been met prior to submitting a Deliverable or Milestone for Acceptance by DIR or a DCS Customer. Acceptance Criteria include: (i) any mutually agreed written criteria identified as Acceptance Criteria, (ii) Compliance, (iii) for all Software and System deliverables that process data, such item successfully integrates with all other Services, Software, Equipment, Systems, and other resources and is fully documented such that the anticipated end user can utilize the functionality of such Deliverable in the manner and for the purpose intended and that reasonable knowledgeable professionals can understand, maintain, support, and modify such Deliverable in accordance with its intended use.
Acceptance Review Period	Has the meaning given in Section <a href="#">10.6 Acceptance Review Period</a> , provided that any provisions of written notice alerting DIR that a Milestone or Deliverable is complete and ready for review that is submitted outside a Business Day shall be considered to be submitted, for the purposes of DIR internal review, on the next Business Day immediately following the day on which such notice was submitted.
ADC	Austin Data Center
ADDF	Application Development Decision Framework – High level information about the ADDF is available at this link: <a href="https://pubext.dir.texas.gov/portal/internal/resources/DocumentLibrary/Texas%20ADDF%20Pamphlet.pdf">https://pubext.dir.texas.gov/portal/internal/resources/DocumentLibrary/Texas%20ADDF%20Pamphlet.pdf</a>
Administration Services	The act of managing planning, directing, and coordinating supportive services for an activity and/or organization.
Affiliate	With respect to an Entity, any other Entity that directly or indirectly Controls, is Controlled by, or is under common Control with that Entity at the time in question.
Agreement (also Master Services Agreement and MSA and Contract)	The final version of any contractually binding agreement between DIR and the Successful Respondent relating to the subject matter of the RFO; references to the Agreement include all Exhibits, Attachments and other documents attached thereto or incorporated therein by reference. Notwithstanding the foregoing, unless expressly provided or the context otherwise requires, references to the Agreement in conjunction with Section or Article references shall be deemed references to the body of the Agreement.
AIMS	Asset Inventory and Management System.
API	Application Programming Interface.

Term	Definition
Appliances	A specialized computing device with pre-integrated and pre-configured hardware and/or software packaged to provide a “turn-key” solution. The computing function in an Appliance, though configurable, is designed by the manufacturer to provide a specific function with little or no support. Computer appliances differ from general purpose computers such as an Application or Infrastructure Server in that they are not designed to be modified. Appliances may be physical or virtual and support a variety of functions.
Applications	All software programs and programming (and all modifications, replacements, Upgrades, enhancements, documentation, materials, media, on-line help documentation and tools related thereto) that perform user or DCS Customer-related information processing functions or support day- to-day operations (including the supporting documentation, media, on- line help facilities, and tutorials), or otherwise used in the provision of Services by Successful Respondent. Applications include all such programs and programming in use or required to be used as of the Commencement Date. Applications also include all such programs and programming developed and/or introduced by or for DIR, any DCS Customer, or Successful Respondent during the Term. Applications do not include the tools, utilities, or Operating Software or Systems Software used to deliver Applications.
Architecture	The design, process, strategies, and specification of the overall structure, logical components, and the logical interrelationships of Equipment and Software, including System Software, a Network, or other reasonably related conception.
Assessment(s) or Assessed	Has the meaning given in Section <a href="#">9.9.11.4 Security Assessments</a> .
Assessment Notice Date	The date that DIR or the Security Assessment Company, as applicable, provides an Assessment report to Successful Respondent.
Asset Inventory and Management System (AIMS)	An automated, database-driven application used to store, query, and maintain asset inventory information for all assets used in association with the Services, whether the assets are located at DIR Facilities or Successful Respondent Facilities. The AIMS provides an inventory of the IT infrastructure managed by the Successful Respondent.
Assistance Event	(i) Any termination (in whole or in part) under, or the expiration of, the Agreement, or (ii) The discontinuance of the provision of the Services (in whole or in part) in respect of any DCS Customer.
At-Risk Amount	For any month during the Term, the percent (%) of the Service Level Invoice Amount, which is the maximum amount that the Successful Respondent will have at risk for Service Level Credits as set forth in <b>Attachment 1.2 Service Level Matrix</b> . Each Service Component will have its own At-Risk Amount tied to the corresponding portion of the Service Level Invoice Amount. See the formula in Section 6.5 of this <b>Exhibit 1</b> .
Audit Period	Has the meaning given in <b>MSA Section 4.11.1 Contract Records</b> .
Authorized Users	Unless otherwise indicated, officers, directors, employees, contractors, agents, customers, and vendors of DIR or any DCS Customer and any other person(s) designated by DIR or any DCS Customer to receive or use the Systems or Services provided by Successful Respondent.
Availability or Available	The full functionality of a Service Component is ready and accessible for use by the Authorized Users and is not degraded in any material respect.
Bankruptcy Code	Has the meaning given in <b>MSA Section 13.5.2 DIR Rights in Event of Bankruptcy Rejection</b> .
Bankruptcy Rejection	Has the meaning given in <b>MSA Section 13.5.2 DIR Rights in Event of Bankruptcy Rejection</b> .

Term	Definition
BAR	Business Analytics and Reporting
BC	Business Continuity.
Business Continuity	The overall enterprise plans and specific activities of each DCS Customer and/or Service Component Provider (SCP) that are intended to enable continued business operations in the event of any unforeseen interruption (e.g., plans and activities to move a department to a new location in the event of a disruption).
Business Day	Each day from Monday through Friday, excluding State holidays, 7:00 a.m. to 5:00 p.m., Local Time. State holidays will include all holidays with the status “All agencies closed.” State holidays will not include State optional holidays or holidays that require skeleton crews. For SLAs related to outbound mail Services, Business Day means each day from Monday through Friday, excluding US postal holidays, 7:00 a.m. to 5:00 p.m., Local Time. For SLA reporting purposes, the hours listed in <b>Attachment 1.3 Service Level Definitions and Performance Analytics</b> would override the 7:00 a.m. to 5:00 p.m.
Cabling	The physical connection between pieces of equipment that are generally loose, not necessarily permanent and attached to infrastructure (e.g. within racks and cabinets).
Call	A contact (including by telephone, voicemail, electronic mail, fax, automated tool or web request) to Successful Respondent reporting a problem, requesting assistance or Services, or asking a question pertaining to the Services, as well as automated alerts and other problem and Service notifications communicated to Successful Respondent.
CAP Failure Credit	Has the meaning given in Section <a href="#">6.8 Service Delivery Failure: Corrective Action Plan</a> .
CDC	Consolidated Data Center (inclusive of both ADC and SDC).
Change Control Procedures	Has the meaning given in <b>MSA Section 4.10 Change Control</b> .
Change Management or Change Management Process	The processes relating to planning and performing all changes in DCS Customer's IT environment pertaining to the Services, including changes to individual components and coordination of changes across all components. The Change Management processes will support and include checkpoints to determine any potential or required Change Control Procedures.
Chargeback	Has the meaning given in <b>Exhibit 2 Pricing</b> .
Chargeback System	The system for Chargeback as described in <b>Section 2.3 of Exhibit 2 Pricing</b> .
Charges	The Monthly Base Charge, Additional Resource Charges and any other amounts payable by DIR to Successful Respondent pursuant to the express terms of the Agreement.
CI	Configuration Items; any component part of Services that is (or is to be) under the control of Configuration Management and therefore subject to formal Change Control.
CJIS	Criminal Justice Information Services
Cloud	Shared pools of configurable computer system resources and higher-level services that can be rapidly provisioned with minimal management effort, often over the Internet. Cloud computing relies on sharing of resources to achieve coherence and economies of scale, similar to a public utility.
CMDB	Configuration Management Database is a database used by an organization to store information about hardware and software assets. This database acts as a data warehouse for the organization and also stores information regarding the relationship between its assets.
CMS	Configuration Management System. A system engineering process for establishing and maintaining consistency of a product's performance, functional, and physical attributes with its requirements, design, and operational information throughout its life.

<b>Term</b>	<b>Definition</b>
Commencement Date	September 1, 2020, or the date the Parties agree upon, in writing, as the date on which Successful Respondent begins providing the Services to the first DCS Customer.
Compliance and Comply	With respect to Deliverables, fulfilling the requirements of the specifications, the Acceptance Criteria, the Agreement, and all other applicable operational and/or functional requirements.
Component	A grouping of software functionally or a separate software object in the solution that has the ability to "stand alone" or "integrate with other components" as required.
Confidential Information	Has the meaning given in <b>MSA Section 6.1.1</b> .
Configuration Management Database (CMDB)	A System that contains details regarding the Software, Equipment and Systems that are used in the provision and management of the Services, including information that relates to the maintenance, movement and problems experienced with such Software, Equipment and Systems.
Connectivity	The ability to access and exchange data, voice, and/or video electronic impulses between various Infrastructure components and with external sources as approved by DIR and provided to Authorized Users.
Consolidated Data Center(s)	Means the centralized Data Center(s) used by Successful Respondent to provide Services (including the ADC and SDC).
Contract Changes	Has the meaning given in Section <a href="#">10.1 Contract Changes</a> .
Contract Records	Has the meaning given in <b>MSA Section 4.12.1</b> .
Contract Year	Each twelve (12) month period commencing each September and ending each August during the Term. If any Contract Year is less than twelve (12) months ("Stub Period"), the rights and obligations under this Agreement that are calculated on a Contract Year basis will be proportionately adjusted for such shorter period.
Contract	See "Agreement".
Control, Controlled and Controlling	Means (a) the legal, beneficial, or equitable ownership, directly or indirectly, of (i) at least fifty percent (50%) of the aggregate of all voting equity interests in an Entity, or (ii) equity interests having the right to at least fifty percent (50%) of the profits of an Entity or, in the event of dissolution, to at least fifty percent (50%) of the assets of an Entity; (b) the right to appoint, directly or indirectly, a majority of the board of directors; (c) the right to control, directly or indirectly, the management or direction of the Entity by contract or corporate governance document; or (d) in the case of a partnership, the holding by an Entity (or one of its Affiliates) of the position of sole general partner. For purposes of this Agreement, a Change in Control under <b>MSA Section 13.3</b> occurs if the ultimate parent entity no longer Controls (as described above) Successful Respondent.
Corrective Action Plan or CAP	See CAP Failure Credit
CPU	Central Processing Unit
Critical Deliverable	Deliverables that have associated Deliverable Credits payable to DIR in the event Successful Respondent fails to successfully and timely complete such Deliverables as identified in the Agreement. For further clarity, successfulness is measured by whether the Deliverables meet the associated Acceptance Criteria.
Critical Milestone(s)	The event(s) that evidence that progress has been made and that specific action(s) has taken place in the advancement of work. Usually viewed as a significant achievement or attainment of a specific goal or sub-goal.

Term	Definition
Critical Service Level	Any Service Level designated as "critical" by DIR, and with respect to which DIR may become entitled to receive Service Level Credits as a result of Successful Respondent's failure to satisfy the associated Service Level standards.
Cross-Functional Services	Those Services performed in connection with performing, and in support of, each of the Services, including those Services described in Article 9, Cross-Functional Services, of this SOW.
CSP	Cloud Service Provider
Data Quality Management (DQM)	The business processes that ensure the integrity of an organization's data during collection, application (including aggregation), warehousing, and analysis.
DCS	Data Center Services
DCS Customer or DIR Customer	Collectively, any of the following Entities that are designated by DIR to receive Services under the Agreement, whether directly from any DCS Service Component Provider or from DIR through an Interagency, Interlocal, or other agreement: (a) DIR in its capacity as a recipient of Services; (b) any State agency, unit of local government or institution of higher education as defined in Section 2054.003, Texas Government Code, and those State agencies that execute Interagency Agreements with DIR, as authorized by Chapter 771, Texas Government Code; (c) any Texas local government as authorized through the Interlocal Cooperation Act, Chapter 791, Texas Government Code; (d) any other state or governmental Entity of another state, as authorized by Section 2054.0565, Texas Government Code; (e) any other Entity permitted under Law to purchase Services from or through DIR; and (f) other Entities to which the Parties agree. The Parties acknowledge and agree that the definition of eligible DCS Customers is subject to modification by the State Legislature, and that the then-current definition of DCS Customers shall control for all purposes.
DCS Governance	Has the meaning given in Article 8 <a href="#">DCS Governance Model</a> .
DCS Network or Managed DCS Network Services	The DCS Service Component providing Network support and services. It is a DCS Shared Technology Service (STS) that will be provided by an SCP. One (1) of several Service Components comprising the DCS Program.
DCS Prospects	Potential Data Center Services clients.
DCS Security Operations Services (SOS)	The DCS Service Component for Security. It is a DCS STS that will be provided by an SCP. One (1) of several Service Components comprising the DCS Program.
DCS Service Component Provider(s)	Collectively, all Service Component Providers and the MSI.
Deliverable	In accordance with Section <a href="#">10.2 Deliverables</a> , a vendor-provided tangible item or outcome that DIR reviews and approves at a specified date/frequency during the term of the contract, excluding reports that are managed/monitored through other defined processes. Deliverables may have certain attributes that impact the review and acceptance. The term includes Recurring and One-Time Deliverables.
Deliverable Credits	Has the meaning given in Section <a href="#">10.10 Deliverables Credits</a> .
Derivative Work	A work based on one or more preexisting works, including a condensation, transformation, translation, modification, expansion, or adaptation, that, if prepared without authorization of the owner of the copyright of such preexisting work, would constitute a copyright infringement under applicable Laws, but excluding the preexisting work.

Term	Definition
Designated DIR Representative	Has the meaning given in <b>MSA Section 5.1.1 Designated DIR Representative</b> .
Developed Material(s)	Any Materials or any modifications, enhancements, improvements, Upgrades or Derivative Works of such Materials that are developed pursuant to the Agreement and paid for by DIR or any DCS Customer under the Agreement. Developed Materials does not include any underlying Successful Respondent or Third Party Owned Materials.
Development or Development Environment	The Systems environment in which Software and databases are initially designed and created. DCS Customers may have more than one Development Environment.
DIR	Department of Information Resources
DIR Auditors	Has the meaning given in <b>MSA Section 4.12.2 Operational Audits</b> .
DIR Business Days	Means weekdays (Monday through Friday) excluding State of Texas and Federal holidays. The term does not include weekends.
DIR Contractor(s)	Has the meaning as the term is used in <b>MSA, Article 4 Services</b> .
DIR Data	<p>Any data or information of or regarding DIR or any DCS Customer that is provided to or obtained by Successful Respondent in connection with the negotiation and execution of the Agreement or the performance of Successful Respondent's obligations under the Agreement, including data and information with respect to the constituency, customer, operations, facilities, products, rates, regulatory compliance, competitors, assets, expenditures, mergers, acquisitions, divestitures, billings, collections, revenues and finances of DIR or any DCS Customer. DIR Data also means any data or information:</p> <ol style="list-style-type: none"> <li>1. created, generated, collected or processed by Successful Respondent in the performance of its obligations under the Agreement, including data processing input and output, service level measurements, asset information, Reports, third party service and product agreements, contract charges, and retained expense and Pass-Through Expenses;</li> <li>2. that resides in or is accessed through Software, Equipment or Systems provided, operated, supported, or used by Successful Respondent in connection with the Services, as well as information derived from this data and information, but excluding the following information to the extent not required to be provided or otherwise made available to DIR under this Agreement, including with in connection with DIR's rights related to Benchmarking, Subcontractors, auditing, Reports, or Termination Assistance Services: financial/accounting information (including costs, expenditures, billings collections, revenues and finances) of Successful Respondent, its Affiliates or Subcontractors;</li> <li>3. information created by Successful Respondent to measure the productivity and efficiency of the Services and/or to improve the processes and procedures used by in the performance of the Services;</li> <li>4. human resources and personnel information of Successful Respondent, its Affiliates or Subcontractors; and</li> <li>5. information with respect to Third Party Contracts or licenses of Successful Respondent, its Affiliates or Subcontractors and used in the performance of the Services.</li> </ol> <p>Data or information constituting DIR Data shall not constitute Successful Respondent Confidential Information.</p>

<b>Term</b>	<b>Definition</b>
DIR Facilities or DIR Facility	The facilities that are provided by DIR or a DCS Customer for use by Successful Respondent to the extent necessary to provide the Services as well as those DIR, DCS Customer and DIR Contractor locations at or to which Successful Respondent is to provide the Services. DIR Facilities include the Non-Consolidated Service Locations and the Consolidated Data Centers.
DIR Laws	Has the meaning given in <b>MSA Section 8.11.4 Notice of Laws</b> .
DIR Owned Materials	Has the meaning given in <b>MSA Section 7.1 DIR Owned and Licensed Materials</b> .
DIR Personal Data	That portion of DIR Data that is subject to any Privacy Laws and includes, but is not limited to, information which any DCS Customer discloses that consists of personal Confidential Information or identifies any consumer served by the Texas Health and Human Services Commission or constituent agencies, in accordance with applicable federal and state laws and other applicable rules, including but not limited to the Texas Health and Safety Code and 25 Texas Administrative Code, Chapter 414.
DIR Project Manager	The person or the person's designee identified by DIR as the responsible individual from DIR to manage the project.
DIR Rules	Has the meaning given in <b>MSA Section 4.4 DIR Rules/Employee Safety</b> .
DIR Standards or Standards	Has the meaning given in <b>MSA Section 4.10 Change Control</b> .
DIR-Initiated Financial Dispute	Has the meaning given in <b>Exhibit 2 Pricing, Section 2.2.4.3</b> .
Disaster	(1) A sudden, unplanned calamitous event causing great damage or loss; (2) any event that creates an inability on an organizations part to provide critical business functions for some predetermined period of time; (3) in the business environment, any event that creates an inability on an organization's part to provide the critical business functions for some predetermined period of time; (4) the period when company management decides to divert from normal production responses (in total or in part) and exercises its disaster recovery plan; and (5) typically signifies the beginning of a move from a primary to an alternate location.
Disaster Recovery (DR) Services	The process of following specific advance arrangements and procedures in response to a disaster, resumption of the critical business functions within a predetermined period of time, minimizing the amount of loss, and repairing or replacing the damaged facilities as soon as possible. The Disaster Recovery Services include support and coordination with the Business Continuity Services.
Disaster Recovery Plan (DRP)	The plan to execute Disaster Recovery Services.
Downtime	The time that a particular System, Application, Software, Equipment, Network or any other part of the Services is not Available during the Measurement Window.
DR	Disaster Recovery
DRP	Disaster Recovery Plan
Earnback	The methodology used to determine the potential return of a Service Level Credit as described in Section <a href="#">6.6 Earnback</a> .
Effective Date	Has the meaning given in the "Authority to Execute" Section of the Agreement (immediately after <b>MSA Section 14.26</b> ), which is understood to be the day the final party signs the Agreement.
Electronic PHI or ePHI	Has the meaning given in <b>MSA, Section 6.3 DIR Personal Data</b> .
Eligible Customer(s)	See DCS Customers.

<b>Term</b>	<b>Definition</b>
Entity or Entities	A governmental body, agency, unit or division (including those categories described in the definition of DCS Customer), corporation, partnership, joint venture, trust, limited liability company, limited liability partnership, association, or other organization or entity.
Equipment	The computer, telecommunications, and facility-related hardware, equipment, and peripherals (and all modifications, replacements, Upgrades, enhancements, documentation, materials, and media related thereto) that are used in connection with the Services provided by Successful Respondent. Equipment includes all such computer, telecommunications, and facility-related hardware, equipment, and peripherals in use or required to be used as of the Commencement Date, including those set forth in the Agreement; those as to which the lease, maintenance, or support costs are included in the Financial Base Case; and those as to which Successful Respondent received reasonable notice and/or access prior to the Commencement Date. Equipment also includes all such computer, telecommunications, and facility-related hardware, equipment, and peripherals purchased or leased by or for DIR, any DCS Customer, or Successful Respondent during the Term.
Equipment Leases	All leasing arrangements whereby DIR, DCS Customers, or any DIR Contractor leases Equipment as of the Commencement Date which shall be used by Successful Respondent to perform the Services after the Commencement Date. Equipment Leases include those leases identified in <b>Exhibit 2 Pricing, Attachment 2.2 Financial Responsibility Matrix</b> , those as to which the costs are included in the Financial Base Case, and those as to which Successful Respondent received reasonable notice and/or reasonable access prior to the Commencement Date. Equipment Leases also include all such leasing arrangements entered into by or for DIR, DCS Customers, any DIR Contractor, or Service Component Provider (SCP) during the Term.
Escrow Agreement	Has the meaning given in <b>MSA Attachment 3 Form of Source Code Escrow</b> .
Event of Loss	Has the meaning given in <b>MSA Attachment 2 Insurance and Risk of Loss</b> .
Expected Service Level	Means the desired level of performance for a Critical Service Level or Key Measurement, as set forth in <b>Attachment 1.3, Service Level Definitions</b> .
Expiration Date	Means the ending date of the Term as used in <b>MSA Section 3.2 Extension</b> .
Extraordinary Event	A circumstance in which an event or discrete set of events has occurred or is planned with respect to the operations of DIR or the DCS Customers that results or shall result in a change in the scope, nature or volume of the Services that DIR or the DCS Customers shall require from Successful Respondent. Examples of the kinds of events that might cause such substantial increases or decreases include the following: (1) changes in locations where the DCS Customers operate; (2) changes in constituencies served by, or activities or operations of, the DCS Customers; (3) privatizations, dispositions, or reorganizations of the DCS Customers; (4) changes in the method of service delivery; (5) changes in the applicable regulatory environment or applicable Laws; and, (6) changes in DIR's or a DCS Customer's policy, technology or processes.
FAQ(s)	Frequently Asked Question. A frequently asked question or list of such questions.
Federal Tax Information (FTI)	Any Federal tax information, including without limitation, and tax return-derived information received from the IRS.
FERPA	Family Educational Rights and Privacy Act
FRA	Fast Recovery Area
FTE	Full Time Equivalent
FTI	Federal Tax Information

Term	Definition
Full Time Equivalent (FTE)	A level of effort, excluding vacation, holidays, training, administrative and other non-productive time (but including a reasonable amount of additional work outside normal business hours), equivalent to that which would be provided by one (1) person working full time for one (1) year. Unless otherwise agreed, one (1) FTE is assumed to be 1,920 productive hours per year. Without DIR's prior written approval, one (1) dedicated individual's total work effort cannot amount to more than one (1) FTE.
Fully Managed Services	The management and responsibility for providing services as defined in <b>Request for Offer (RFO) Section 1.3.1.</b>
Governance Model	Has the meaning given in Article <a href="#">8</a> DCS Governance Model.
Hardware Service Charge (HSC)	Has the meaning given in <b>Exhibit 2 Pricing, Section 2.3.</b>
HCI	Hyper Converged Infrastructure. A software-defined IT infrastructure that virtualizes all of the elements of conventional "hardware-defined" systems.
Help Desk	The facilities, associated technologies, and fully trained DCS Customer staff who respond to calls, coordinate all problem and request management activities, and act as a single point of contact for end users.
HIPAA	Health Insurance Portability and Accountability Act
Historically Underutilized Business(es)	The meaning given to such term by the Texas Comptroller of Public Accounts.
HSC	See Hardware Services Charge.
HUB	Historically Underutilized Business
I/P/C	Incident, Problem, and Change
IaaS	Infrastructure as a Service
IIRIRA	Has the meaning given in <b>MSA Section 8.7 Certifications.</b>
Incident	An event which is not part of the standard operation of a Service and which causes or may cause disruption to or a reduction in the quality of Services and DIR and/or DCS Customer productivity.
Income Tax	Any tax on or measured by the net income of a Party (including taxes on capital, net worth or revenue that are imposed as an alternative to a tax based on net or gross income), or taxes which are of the nature of excess profits tax, minimum tax on tax preferences, alternative minimum tax, accumulated earnings tax, personal holding company tax, capital gains tax, or franchise tax for the privilege of doing business.
Incumbent Personnel	Employees of the Incumbent SCP(s) or their subcontractors providing Services to DIR pursuant to the terms of a MSA by and between DIR and the Incumbent SCP(s).
Incumbent Service Component Provider(s)	The vendor or their subcontractors providing Services to DIR pursuant to the terms of the MSA by and between DIR and the vendor. Generally speaking, the Incumbent Service Component Provider for DCS is Atos.
Information Technology Infrastructure Library (ITIL)	A world-wide recognized best-practice framework for the management and delivery of IT services throughout their full lifecycle. The primary structure of the requirements in the Statements of Work are based on an ITIL v2 Foundations with ITIL v3 guidance in select functional areas (e.g., Request Management and Fulfillment) with the expectation of migrating towards ITIL v3 progressively as process improvements are incorporated into the Service Management Manual.

Term	Definition
Infrastructure	The entire portfolio of Equipment, System Software, and Network components required for the integrated provision and operation of DIR and DCS Customer's IT Systems and Applications.
In-Scope	Those Services or resources that are the subject of Successful Respondent's obligations under the Agreement.
IRS	Internal Revenue Service. A division of the U.S. Treasury Department responsible for collecting taxes.
ITIL	See Information Technology Infrastructure Library
ITSCM	IT Service Continuity Management. Aims to manage risks that could impact IT services.
ITSM	Information Technology Service Management. Describes a strategic approach to design, deliver, manage, and improve the use of IT.
Key Personnel	Has the meaning given in Section 5 Successful Respondent Personnel Requirements.
KSL	Key Service Level
Laws	All federal, state and local laws, statutes, ordinances, regulations, rules, executive orders, circulars, opinions, interpretive letters and other official releases of or by any government, or any authority, department or agency thereof.
Legacy Modernization Guide	The guide created by DIR to provide guidelines, principles, best practices and references for developing a plan to modernize a legacy environment. At the time of the Effective Date, the guide is located at this location: <a href="https://pubext.dir.texas.gov/portal/internal/resources/DocumentLibrary/Legacy%20Modernization%20Guide.pdf">https://pubext.dir.texas.gov/portal/internal/resources/DocumentLibrary/Legacy%20Modernization%20Guide.pdf</a>
Level 1 Support	Support that is provided as the entry point for inquiries or problem reports from Authorized Users. If Level 1 personnel cannot resolve the inquiry or problem, the inquiry or problem is directed to the appropriate Level 2 personnel or a Third Party for resolution.
Level 2 Support	Support that serves as a consolidation point for inquiries and problems. For example, Level 2 Support might exist in a computer operation or a distribution/mail out center. If Level 2 personnel cannot resolve the inquiry or problem, the inquiry or problem is directed to the appropriate personnel or a Third Party for resolution.
Local Time	Central Standard Time or daylight savings time, as is then prevailing, in Austin, Texas.
Logical Security	Controlling access to information, software, and data by utilizing Operating Software parameters and Applications-level security controls. Logical Security includes logical separation of processors and disk and segregation of reusable storage media.
Losses	All losses, liabilities, damages (including punitive and exemplary damages), fines, penalties, settlements, judgments, interest and claims (including taxes), in each case that a court finally awards to a third party or which are otherwise included in the amount payable to a third party and all related costs and expenses (including reasonable legal fees and disbursements and costs of investigation, litigation, experts, settlement, judgment, interest and penalties), as incurred.
Mainframe Service Component Provider	The DCS SCP who has entered into a contract with DIR for the Mainframe Statement of Work. One (1) of eight (8) Service Components comprising the DCS Program within STS.
Major Incident	The highest category of impact for an Incident. A Major Incident results in significant disruption to business operations.

Term	Definition
Malicious Code	(i) Any code, program, or sub-program whose knowing or intended purpose is to damage or interfere with the operation of the computer system containing the code, program or sub-program, or to halt, disable or interfere with the operation of the Software, code, program, or sub-program, itself, or (ii) Any device, method, or token that permits any person to circumvent the normal security of the Software or the system containing the code.
Management Tools	All items used by Successful Respondent to deliver and manage the Services, including but not limited to software products and tools, code, scripts, bots, automation, and any and all methods, processes, inventions, machines, compositions, know-how, and show-how related thereto (and all modifications, replacements, Upgrades, improvements, enhancements, documentation, materials and media related thereto). Management Tools shall include all such products and tools in use or required to be used as of the Commencement Date, including those set forth in <b>Attachment 1.3 Service Level Definitions and Performance Analytics, Section 2.4</b> , those as to which the license, maintenance, or support costs are included in the Financial Base Case, and those as to which Successful Respondent received reasonable notice and/or access prior to the Commencement Date. Management Tools also shall include all such products and tools selected and/or developed by or for DIR, any DCS Customer or Successful Respondent during the Term.
Marketplace	A type of e-commerce site where product or service information is provided by multiple third parties, whereas transactions are processed by the marketplace operator.
Materials	All tangible and intangible items and property, including but not limited to code; tools; scripts; bots; automation; formulae; algorithms; processes; process improvements; procedures; designs; concepts; inventions; machines; articles of manufacture; compositions; improvements; methodologies; trade secrets; technology; Software (in both object and source code form); databases; specifications; configurations; any all methods, process, inventions, machines, compositions, know-how, and show-how related thereto; and all records thereof, including documentation, design documents and analyses, interface documentation, studies, tools, plans, models, flow charts, reports and drawings.
MDS	Master Data Services. A Master Data Management product from Microsoft that ships as a part of the Microsoft SQL Server relational database management system. Master Data Services is the SQL Server solution for master data management.
MDSS or SDS or MSDS	Material Data Safety Sheet, or a Safety Data Sheet, or a Material Safety Data Sheet. A document that lists information relating to occupational safety and health for the use of various substances and products.
Measurement Window	The time during, or frequency by, which a Service Level shall be measured. The Measurement Window will exclude approved scheduled maintenance.
Middleware	Software that facilitates interactions and integration between and among two (2) or more separate Software programs, Systems, or platforms.
MIM	Major Incident Management. The management of a Major Incident which demands a response beyond the routine incident management process.
Minimum Service Level	The minimum level of performance set forth in <b>Exhibit 1 SOW, Attachment 1.2 Service Level Matrix</b> with respect to each Service Level.
Monthly Charges	The total Charges invoiced by Successful Respondent in any calendar month for Services (excluding Pass-Through Expenses, Out-of-Pocket Expenses and Service Taxes). See <b>Exhibit 2 Pricing, Section 3.2</b> .
Monthly Invoice	Has the meaning given in <b>Exhibit 2 Pricing , Section 2.2.1.1</b> .

Term	Definition
Monthly Productive Hours Worked	With respect to any month and any Successful Respondent Personnel, the number of productive hours worked by such Successful Respondent Personnel, excluding non-productive time (e.g., commuting time, vacation, holidays, training unrelated to the Services, education, marketing, administrative staff meetings, medical leave, and military leave).
Multi-sourcing Services Integrator (MSI)	The Service Component Provider who has entered into a contract with DIR for Multi-sourcing Services Integrator services.
MSI Portal	The MSI provided online portal for SCPs, Customers and DIR to use to communicate, request services and manage the services.
Multi-Supplier Environment	Has the meaning given in Section <a href="#">9.2</a> Multi-sourcing Services Integration and Cooperation.
N/N-1	The version of Software designated and/or approved by DIR or the applicable governance committee, as the current standard for deployment. N-1 is one (1) release prior to the above-described designated or approved Software version.
NAS	Network Attached Storage
Network Topology	The arrangement in which the nodes or interfaces to the Network are connected.
New Services	Services requested by DIR, DCS Customers, or required by applicable Laws (without limiting the obligation of the Parties under <b>MSA Section 8.11 Compliance with Law</b> ) (i) that are materially different from the Services, (ii) that require materially different levels of effort or resources from Successful Respondent to provide the Services, and (iii) which are not required for Successful Respondent to meet the Service Levels. For the avoidance of doubt, New Services shall not include (a) increases in the volume of Services for which there is an associated Resource Baseline or charging methodology, or (b) the disaggregation of an existing service from a Functional Service Area.
NIST	National Institute of Standards and Technology
Noncompliance	Each instance that the Software, Equipment, Systems, or other Deliverable or milestone fails to meet its Acceptance Criteria or is otherwise deficient in DIR's reasonable discretion (in accordance with the SMM or other criteria agreed by the Parties, to the extent applicable).
Non-consolidated Compute	Includes service locations outside of the DIR CDCs as well as remote sites where break-fix services will also be performed.
Notice of Election	Has the meaning given in <b>MSA Section 10.3.1 Notice</b> .
OEM	Original Equipment Manufacturer
One-Time Charges	Any Charges that are specified by the Successful Respondent and which are non-recurring and are typically associated with start-up and implementation costs.
One-Time Deliverables	Those Deliverables that are non-recurring that have associated Deliverable Credits payable to DIR in the event Successful Respondent fails to successfully and timely complete such Deliverables.
Operating Level Agreements (OLA)	Has the meaning given in <b>MSA Section 4.1 Overview</b> .
OS	Operating System
Outage	A condition such that a System, Service, Application System, Equipment or network component is not Available or is substantially not Available and is impacting normal business operations.

Term	Definition
Out-of-Pocket Expenses	Reasonable, demonstrable and actual expenses due and payable to a Third Party by Successful Respondent that are approved in advance by DIR and for which Successful Respondent is entitled to be reimbursed by DIR under the Agreement. Out-of-Pocket Expenses shall not include Successful Respondent's overhead costs (or allocations thereof), general and/or administrative expenses or other markups. Out-of-Pocket Expenses shall be calculated at Successful Respondent's actual incremental expense and shall be net of all rebates and allowances.
Party(ies)	Has the meaning given in the recitals to the Agreement.
Pass-Through Expense(s)	The Successful Respondent expenses identified in <b>Exhibit 2 Pricing, Section 3.7</b> of which DIR has agreed to pay directly or reimburse to Successful Respondent on an Out-of-Pocket Expenses basis.
Payment Deliverables	Those Deliverables that have associated payments due to the Successful Respondent after DIR approval of such Deliverables. Payment will be provided in accordance with the Agreement.
PCI DSS	Payment Card Industry Data Security Standard has the meaning given in <b>MSA Section 6.5.4 Cardholder Data</b> .
PDU	Power Distribution Unit
Penetration Tests	A type of Assessment that tests the vulnerability of Systems to unauthorized external interventions or improper uses.
Performance Category	A grouping of Critical Service Levels or Key Measurements. Critical Deliverables do not constitute a Performance Category.
PII	Personally Identifiable Information. Any data that could potentially identify a specific individual.
Plan	Has the meaning given in <b>MSA Section 6.3</b> .
Portal	The online Internet site providing access and links to Services and other applications.
PPM	Project and Program Management
Print-Mail Component Provider	The DCS SCP who has entered into a contract with DIR for the Print-Mail Statement of Work.
Privacy Laws	Laws relating to data privacy or data protection.
Problem	An underlying cause of one (1) or more Incidents. A Problem is labeled a "Known Error" when the root cause is known and a temporary workaround or permanent solution has been identified.
Privileged Access	Any accounts that have escalated or administrative privileges. The ability to make back end, network, database, or Operating System configuration changes. Example account types: Root, Data Base Administrator, Administrator
Problem Management	The process of tracking and managing all problems arising in DIR and DCS Customer's IT environment, and resolving those problems arising from or related to the Services.
Production or Production Environment	The system environment in which an organization's data processing is accomplished. This environment contains DCS Customers' business data and has the highest level of security and availability of all environments (includes training and other Production-like environments).
Project Manager (Successful Respondent's)	The person or the person's designee identified by the Successful Respondent as the responsible individual from the Successful Respondent's organization to manage the project.
Project(s)	Means discrete units of work approved by DIR, undertaken to create a unique product or result.
Proposal	Has the meaning given in the preamble to the Agreement.

Term	Definition
Protected Health Information (PHI)	Has the meaning given in <b>MSA Section 6.3 DIR Personal Data.</b>
Public Cloud	Computing services offered by third-party providers where scalable and elastic capabilities are provided as a service to customers using Internet technologies.
Public Information Act	Has the meaning given in <b>MSA Section 6.1.2 Disclosure of Confidential Information.</b>
QAT	Quality Assurance Team has the meaning set forth in Section <a href="#">9.9.16 Project Management</a> .
Quality Assurance (QA)	The actions, planned and performed, to provide confidence that all processes, Systems, Equipment, Software, and components that influence the quality of the Services are working as expected individually and collectively.
RAS	Remote Access Server
Recovery Point Objective (RPO)	Recovery Point Objectives, as designated in Section <a href="#">9.9.13 IT Service Continuity Management Requirements</a> expressed as the acceptable amount of data loss measured in time prior to an event that has been declared as a disaster.
Recovery Time Objective (RTO)	Recovery Time Objectives, as designated in Section <a href="#">9.9.13 IT Service Continuity Management Requirements</a> , expressed as the duration of time within which an Application, including all technology components included in the DCS Customer DR Plan must be recovered, restored and operational starting from the time of declaration of a disaster.
Recurring Deliverables	Those Deliverables to be provided on a scheduled and recurring basis that have associated Deliverable Credits payable to DIR in the event Successful Respondent fails to successfully and timely complete such Deliverables.
Refresh	The upgrading and/or replacing of Equipment and Software during the Term.
Reports	Has the meaning given in Section <a href="#">6.4.1 Reports</a> .
Request Management	The process of tracking and managing all requests from Authorized Users arising in DIR's and DCS Customers' IT environment, and resolving those requests arising from or related to the Services.
Required Consent(s)	<p>The consents (if any) required to be obtained:</p> <ul style="list-style-type: none"> <li>to assign or transfer to Successful Respondent DIR licensed Third Party Materials, Third Party Contracts, Equipment Leases or Acquired Assets (including related warranties).</li> <li>to grant Successful Respondent the right to use and/or access the DIR licensed Third Party Materials, Third Party Contracts, and DIR Provided Equipment in connection with providing the Services.</li> <li>to grant DIR, the DCS Customers and/or their designee(s) the right to use and/or access the Successful Respondent Owned Materials, Third Party Materials and Equipment acquired, operated, supported, used, or required to be used by Successful Respondent in connection with providing the Services.</li> <li>to assign or transfer to DIR, the DCS Customers and/or their designee(s) any Developed Materials to the extent provided in the Agreement.</li> <li>to assign or transfer to DIR, the DCS Customers and/or their designee(s) Successful Respondent Owned Materials, Third Party Materials, Third Party Contracts, Equipment leases or other rights following the Term to the extent provided in the Agreement.</li> <li>all other consents required from third parties in connection with Successful Respondent's provision of, and DIR's and the DCS Customers' receipt and use of, the Services and Successful Respondent's performance of its obligations hereunder.</li> </ul>

<b>Term</b>	<b>Definition</b>
Resolution Time	The amount of time between the Start Time for an Incident and the time such Incident is Resolved.
Resolve or Resolution	The restoration of full Service or the completion of the Service Request in a manner acceptable to DIR or the applicable Authorized User in their reasonable discretion. Resolution may include the restoration of full Service by workaround or other alternative means.
Resource Unit (RU)	A measurable device, unit of consumption, or other unit or resource utilization associated with the Services, as described in <b>Exhibit 2 Pricing</b> , that is used for purposes of calculating Charges.
Resource Unit Category	A category of Resource Units which are measured and with respect to which charging rates or other charging mechanisms apply.
Respondent	A firm, company, entity or individual that responds to the solicitation. Unless the Contract clearly indicates otherwise, all terms and conditions of the Contract that refer to Respondent apply with equal force to Successful Respondent.
Response	Has the meaning given in the recitals of the Agreement.
Response Time	The elapsed time between the time one (1) event occurs such as when a call is placed or received and the time Successful Respondent responds to the event.
Retained Expense(s)	The expense types or amounts retained by DCS Customers as set out in <b>Exhibit 2 Pricing, Section 2.1.1.6</b> .
Retained Systems and Processes	Those systems and processes of DIR or a DCS Customer for which Successful Respondent has not assumed responsibility under the Agreement (including those provided, managed, operated, supported and/or used on their behalf by DIR Contractors). Retained Systems and Processes include equipment and software associated with such systems and processes.
RFO	Request for Offer
RMAN	Recovery Manager
ROM	Rough Order of Magnitude
Root Cause Analysis (RCA)	The formal process, specified in the SMM, to be used by Successful Respondent to diagnose the underlying cause of problems at the lowest reasonable level so that effective corrective action can be taken.
RPO	See Recovery Point Objective.
RTO	See Recovery Time Objective.
SAN	Storage Area Network
SCP	Service Component Provider
SDC	San Angelo Data Center
Security	Means of safeguarding and controlling access to information, software, and data by utilizing policies, procedures and actions, including operating software parameters and applications-level security controls. Security includes logical separation of processors and disk and segregation of reusable storage media.
Security Assessment Company	Has the meaning given in Section <a href="#">9.9.11.4 Security Assessments</a> .
Security Plan	Has the meaning given in Section <a href="#">9.9.11 Information Security Management Requirements</a> .
Security Program	Has the meaning given in Section <a href="#">9.9.11.4 Security Assessments</a> .
Security Software	Has the meaning given in <b>Exhibit 2 Pricing, Attachment 2.2 Financial Responsibility Matrix, Network Tab</b> .

Term	Definition
Server	Any computer that provides shared processing or resources (e.g., Application processing, database, mail, proxy, firewalls, backup capabilities, print, and fax services) to Authorized Users or other computers over the Network. A Server includes associated peripherals (e.g., local storage devices, attachments to centralized storage, monitor, keyboard, pointing device, tape drives, and external disk arrays) and is identified by a unique manufacturer's serial number.
Service and Services	Has the meaning given in <b>MSA, Article 4 Services</b> .
Service Component	A single area which is represented with a Statement of Work (SOW) (i.e., Texas Private Cloud, Managed DCS Network, Security Operations Services, etc.).
Service Component Providers (SCPs)	Means, collectively, all Service Component Providers, excluding the MSI, who have entered into an agreement with DIR to provide the services required by one (1) or more Service Component Statement(s) of Work.
Service Delivery Failure	Has the meaning given in Section <a href="#">6.8 Service Delivery Failure: Corrective Action Plan</a> .
Service Desk	The facilities, associated technologies, and fully trained staff who respond to Calls, facilitate all Incident Management, Problem Management, Change and Request Management activities, and act as a single point of contact for coordination and communication to Authorized Users and SCPs in regard to the Services.
Service Level Credit Allocation Percentage	The percentage of the Allocation of Pool Percentage allocated to a Critical Service Level within a Performance Category.
Service Level Credit Start Date	The period beginning ninety (90) days after the Commencement Date wherein Successful Respondent will be liable for Service Level Credit(s) or CAP Failure Credit(s).
Service Level Credits	The monetary amounts that the Successful Respondent shall be obligated to pay to DIR (or apply against Monthly Charges) in the event of Service Level Defaults.
Service Level Default	Occurs when a Minimum Service Level has not been met.
Service Level Invoice Amount	Charges due and owing for the preceding month, including the Monthly Base Charge and any additional Charges, including, to the extent applicable, any other amounts payable by DIR to Successful Respondent pursuant to the express terms of the Agreement (excluding payments for Transition Milestones Transformation Milestones, and HSC/SSC Charges).
Service Level(s)	Individually and collectively, the quantitative performance standards for the Services set forth in <b>Exhibit 1 SOW, Attachment 1.2 Service Level Matrix</b> and in <b>Exhibit 1 SOW, Attachment 1.3 Service Level Definitions of the Agreement</b> .
Service Management Manual (SMM)	The management procedures manual for the Services as described in <b>Exhibit 1 SOW, Attachment 1.4 SMM Content and Organization</b> .
Service Request (or Request for Service)	A request for information, advice, access, or standard change to an IT service that does not require solution proposal development. Examples of such Service Request include provisioning ID access, password resets, and Service Catalog requests.
Service Taxes	All sales, use, excise, and other similar taxes that are assessed against either Party on the provision of the Services as a whole, or on any particular Service received by DIR or the DCS Customers from SCPs, excluding Income Taxes.
Severity Level	The categorization of a problem associated with the Services based on the potential impact of the problem to DIR and any DCS Customer, as further defined in <b>Exhibit 1 SOW, Attachment 1.3 Service Level Definitions and Performance Analytics, Section 1.1</b> .
SLAs	Service Level Agreements

<b>Term</b>	<b>Definition</b>
SMM	Service Management Manual
Software	All Materials consisting of software programs and programming (and all modifications, replacements, Upgrades, enhancements, documentation, materials and media related thereto), including Antivirus Software, Application Software, Development Tools, and System Software.
Software Service Charge (SSC)	Has the meaning given in <b>Exhibit 2 Pricing, Section 2.3.</b>
Solution Request or Request for Solution	A Service Request that requires development of a proposal for DCS Customer approval to fulfill the request.
SOW	Statement of Work
Specialized Services	Has the meaning given in <b>MSA Section 4.11 Access to Specialized Successful Respondent Skills and Resources.</b>
Specifications	Means, with respect to processes, Software, Equipment, Systems or other contract deliverables to be designed, developed, delivered, integrated, installed, and/or tested by Successful Respondent, the technical, design and/or functional specifications set forth in Third Party Vendor documentation, in a New Services or Project description requested and/or approved by DIR, or otherwise agreed upon in writing by the Parties.
SQL	Structure Query Language
SRT	Schedules, Retentions, and Targets document
SSA	Social Security Administration
SSC	Software Service Charge.
SSMS	SQL Server Management Studio
Staffing Plan	Has the meaning given in Sections <a href="#">2.5.2</a> , <a href="#">2.5.9</a> , <a href="#">5</a> , <a href="#">5.3.1</a> and <a href="#">5.5</a> .
Standard of Due Care	Then-current accepted industry best practices for network and data security that are employed by members of the Peer Group.
Start Time	With respect to an Incident or a Call, the time when the Incident ticket is created. With respect to an Outage, the earlier of the time when the Incident is detected or should have been detected (by the applicable monitoring for the System). If more than one (1) ticket is created for the same root cause, the Start Time shall be based on the earliest of the ticket creation times.
State Data Center(s)	The State data center in San Angelo, Texas, or Austin, Texas.
State Legislature	The governmental legislative body of the State.
State or State of Texas	The State of Texas, unless expressly stated otherwise.
Statement(s) of Work (SOW)	Means this document, Exhibit 1 SOW, and its attachments and appendices.
Strategic Plans	The plans that may be periodically developed by DIR that set forth DIR's key operational objectives and requirements and outline its strategies for achieving such objectives and requirements. DIR may revise the Strategic Plan from time to time. The Strategic Plan is likely to include both annual and multi-year strategies, objectives, and requirements.
Subcontract	An agreement between the Successful Respondent and their Subcontractor(s).
Subcontractor(s)	Subcontractors (of any tier) of Successful Respondent, including Affiliates of Successful Respondent performing Services under the Agreement pursuant to <b>MSA Section 4.13 Subcontractors.</b>
Successful Respondent	The Party to this Agreement.

Term	Definition
Successful Respondent Personnel	Those employees, representatives, contractors, subcontractors, and agents of Successful Respondent and its Subcontractors.
System(s)	An interconnected grouping of manual or electronic processes, including Equipment, Software and associated attachments, features, accessories, peripherals and cabling, and all additions, modifications, substitutions, Upgrades or enhancements to such System. Systems include all Systems in use or required to be used as of the Commencement Date, all additions, modifications, substitutions, Upgrades, or enhancements to such Systems and all Systems installed or developed by or for DIR, the DCS Customers or Successful Respondent during the Term.
Technology Evolution	Any improvement, upgrade, addition, modification, replacement, or enhancement to the standards, policies, practices, processes, procedures, methods, controls, scripts, product information, technologies, architectures, standards, equipment, software, systems, tools, products, transport systems, interfaces and personnel skills available to provide the Services in line with the best practices of first tier leading providers of services that are the same as or similar to the Services. Technology Evolution includes, as relating to such items for such purpose: higher capacity, further scaling and commercializing of processes, more efficient and scalable processes, new versions and types of applications and systems/network software, new operational or IT Infrastructure processes, and new types of hardware and communications equipment that shall enable Successful Respondent to perform the Services more efficiently and effectively as well as enable DIR and the DCS Customers to meet and support their operational requirements and strategies.
Technology Plan	Has the meaning given in Section <a href="#">3.1.3 Technology Planning</a> .
Technology Solution Services	The Services detailed in this Agreement.
Term	The Initial Term and the Renewal Terms, if any, including any period during which Termination Assistance Services are provided by Successful Respondent under the Agreement.
Termination Assistance Services	(i) The Services (including the terminated, insourced, resourced or expired Services, the Services described in <b>MSA Section 7.6</b> of the Agreement and throughout Article <a href="#">11</a> of this SOW and, in each case, any replacements thereof or supplements thereto), to the extent DIR requests such Services during a Termination Assistance Services period; (ii) Successful Respondent's cooperation with DIR, DCS Customers and their designee(s) in the orderly transfer of the Services (or replacement or supplemental services) to DIR, the DCS Customers and/or their designee(s); and (iii) any New Services requested by DIR in order to facilitate the transfer of the Services (or replacement or supplemental services) to DIR, the DCS Customers and/or their designee(s).
Termination Charge	The termination charges payable by DIR as set forth in <b>MSA Section 13.10.2 Termination Charges</b> . The Termination Charge shall be calculated as of the later of (i) the end of the Term (or the date of termination of the applicable Services under the Agreement), and (ii) the satisfactory completion of all Termination Assistance Services.
Texas Data Centers Services (or Data Center Services, DCS)	A program administered by DIR providing Compute and Print/Mail services to eligible DCS Customers.
Third Party Contract(s)	All agreements between Third Parties and DIR, any DCS Customer, or Successful Respondent that have been or shall be used to provide the Services.

Term	Definition
Third Party Materials	Materials that are owned by Third Parties and provided under license or lease to Successful Respondent, DIR or any DCS Customer and that have been or shall be used to provide or receive the Services. Third Party Materials shall include Materials owned by Subcontractors (excluding Affiliates of Successful Respondent) and used in the performance of the Services.
Third Party Vendor(s)	A Third Party that provides products or services to any Party that is related to, or is in support of, the Services (e.g., hardware vendors, premier support contracts, etc.). Third Party Vendors do not include Subcontractors.
Third Party(ies)	A legal entity, company, or person(s) that is not a Party to the Agreement and is not an Affiliate of a Party.
Time-critical (regarding Deliverables)	Deliverables with an expedited review period of five (5) Business Days, designated with a “T”. This is further detailed in Sections <a href="#">10.2 Deliverables</a> , <a href="#">10.6 Acceptance Review Period</a> , and <a href="#">10.7 Noncompliance</a> .
TQM	Total Quality Management
TR&R	Technology Refresh and Replenishment
Transformation Services	The consolidation activities, functions and deliverables, and the implementation of the technology and other process changes, described in the transformation plan.
Transition	Includes all transition activities and deliverables to be completed and provided by Successful Respondent in connection with the migration to Successful Respondent’s Services, and the dates by which each is to be completed by Successful Respondent as further defined in Section <a href="#">2 Transition Services</a> .
Transition and Transformation Charges	Has the meaning given in <b>Exhibit 2 Pricing, Attachment 2.1 Pricing and Volumes</b> .
Transition Milestones	Has the meaning given in <b>Exhibit 2 Pricing, Section 3.5.2</b> .
Transition Plan (also Transition Project Plan)	The plan set forth in Section <a href="#">2.5 Transition Project Plan</a> and developed and updated pursuant to Section <a href="#">2.5.2 Transition Project Plan Critical Deliverable</a> , which identifies all material transition activities and deliverables to be completed and provided by Successful Respondent in connection with the migration to Successful Respondent of the Services, and the dates by which each is to be completed by Successful Respondent.
Transition Services	The transition activities, functions and deliverables described in the Transition Plan and such other tasks as are necessary to enable Successful Respondent to provide the Services.
Transport	A commercial service providing the carriage or transmission of voice, video, or data electronic impulses over a distance.
TRG	Technical Recovery Guide
TSG	Technology Solutions Group
TSLAC	Texas State Library and Archives Commission
TSM	Tivoli Service Manager
TSS	Technology Solution Services.
Type R Service Levels	Type R Service Levels are related measures shared between the MSI and the SCP(s) as defined in Section <a href="#">6.3 Shared and Related Service Levels and Types</a> .
Type U Service Levels	Type U Service Levels are intended to measure Services that are specific to one (1) DCS SCP’s performance, and therefore are not shared between DCS SCPs as defined in Section <a href="#">6.3 Shared and Related Service Levels and Types</a> .

Term	Definition
Unanticipated Change	A material change in the technologies and/or processes available to provide all or any portion of the Services which is outside the normal evolution of technology experienced by the Services, that was not generally available as of the Effective Date and that would materially reduce Successful Respondent's cost of providing the Services.
Upgrade(s)	Updates, patch installations, modifications, renovations, refreshes, enhancements, additions, substitutions and/or new versions or releases of Software or Equipment. For purposes hereof, a workaround or fix to Software or Equipment also constitutes an Upgrade.
UPS	Uninterruptable Power Supply
Use	To load, access, execute, use, manipulate, practice, process, make, have made, operate, copy, execute, compile, store, purge, reproduce, display, perform, distribute, transmit, receive, modify, maintain, enhance, upgrade, store, create Derivative Works, and exercise any other similar rights; provided however that with respect to Third Party Materials that are Software, unless otherwise permitted under the applicable license agreement, the term "Use" shall not include the right to modify or create Derivative Works.
VESDA	Very Early Smoke Detection Apparatus
Virtual Data Center (VDC)	Means a logical environment representing a dedicated networking and security configuration for a specific DCS Customer.
VLANs	Virtual Local Area Networks
VM	Virtual Machine
VMDK	Virtual Machine Disk
VOC	Volatile Organic Compound
VOIP	Voice Over IP
VPN	Virtual Private Network
WBS	Work Breakdown Structure
Wide Area Network (WAN)	A long-haul, high-speed backbone transmission Network, consisting of WAN Equipment, Software, Transport Systems, Interconnect Devices, and Cabling that, and other services as they become available that are used to create, connect, and transmit data, voice and video signals, between or among: (i) LANs, and (ii) other locations that do business with the State and for which DIR is responsible for allowing Connectivity.
Wiring	Wiring that is generally permanent and embedded in the facility. Choices in cost and implementation are often driven by standards for the facility (BICSI or ANSI/TIA or other low-voltage standards specifying such things as plenum or non-plenum, UTP, Cat-6e, etc.). Wiring installation often calls for certifications. Wiring installation often requires physical changes in the building (e.g., boring through walls or flooring) to be done in coordination with the building management.
Work Order	Has the meaning given in the Agreement.
Work Product	(i) All reports and manuals, including Transition Plans, Transformation Plans, business requirements documents, design documents, manuals, training and knowledge transfer materials and documentation, (ii) the Service Management Manual, (iii) Desktop Procedures, and (iv) any literary works and other works of authorship created under the Agreement that express, embody or execute or perform a function, method or process that is specific to the business of DIR or DCS Customers. Work Product includes customized reports, manuals and forms, but not the original unmodified versions used by Successful Respondent as a starting point for creating the customized version.

**NOTE:** Definitions in this table are applicable to all Exhibits and Attachments making up the Public Cloud Manager Request for Offer and subsequent Contract. Pricing-specific definitions are found in **Exhibit 2 Pricing** documents.

## 1. Business Background and Objectives

### 1.1. Background Overview

- (a) The Department of Information Resources (DIR) has established the owner-operator governance model for DIR's current Shared Technology Services (STS) programs, which currently include:
  - (i) Data Center Services (DCS);
  - (ii) Managed Application Services (MAS);
  - (iii) Managed Security Services (MSS); and
  - (iv) Texas.gov.
- (b) The DCS and MAS programs will be restructured to include the following service programs:
  - (i) Texas Private Cloud (TPC)
  - (ii) Public Cloud Manager (PCM)
  - (iii) DCS Security Operations
  - (iv) Network
  - (v) Mainframe
  - (vi) Print, Mail, and Digitization
  - (vii) Technology Solution Services (TSS)
- (c) This model involves DIR and DCS Customers at all levels in governance decision making, including as representatives on all governance committees. The owner-operator model focuses on resolving issues at the lowest possible level and driving for consensus-based solutions. Where consensus cannot be reached, processes include an escalation path. The Successful Respondent will participate and work within the DCS Governance model as it relates to the requirements in the Contract.

### 1.2. Multi-sourcing Service Integrator (MSI)

- (a) DIR leverages an MSI whose role is to integrate and manage the services of the SCPs for the various services of the DCS program, as well as other shared technology services offered by DIR. At a high level, functions provided by the MSI include, but, are not limited to:
  - (i) Service Level Management;
  - (ii) Service Desk Support;
  - (iii) Program Management;
  - (iv) Performance Management
  - (v) Disaster Recovery Testing and Planning;
  - (vi) Financial Management; and
  - (vii) Data Quality and Operational Intelligence.
- (b) The Successful Respondent will actively work with the MSI to provide Services to DIR and DCS Customers through the Contract term. Cross-functional and integration requirements applicable to the Successful Respondent's delivery of Services are outlined in Section 9 [Cross Functional Services](#)
- (c) DIR currently owns licenses for ServiceNow Cloud Management Module and has implemented for Billing and CMDB updates, but have not yet completed Provisioning automation using this toolset. Because the MSI provides core cross-functional services, SCPs shall not duplicate these services; therefore, in its Response, Respondent should identify those services provided by the MSI that would result in cost reductions for the SCP as a result of not providing said services.

### 1.3. PCM Scope and Eligible Customers

Today, there is a current incumbent who delivers management of some Public Cloud hosted instances. Some environment is also managed by the DCS Customer themselves. The services listed herein are available only to DCS Customers or potential Customers hosting workload in the Public Cloud. The Successful Respondent will assume these services upon Contract Commencement.

### 1.4. Service Objectives

The following is a summary of the Service objectives contained within the requirements and scope of this Exhibit:

#### Business Agility

Positioning Texas to utilize DCS public cloud services and adjacent services (e.g., networking, security/privacy – contained in other DCS Program RFOs) to drive innovation for State Agencies and DCS Customers.

#### Collaborative Solutioning

Engaging DCS Customers (and prospects) early in their systems planning cycles to collaborate on driving the best value from DCS public cloud assets and capabilities – whether it be a new opportunity, legacy replacement, systems optimization, technology refresh or re-platforming initiative. May work in conjunction with other DCS SCPs, such as Technology Solutions Services (TSS).

#### Cost & Investment Model

Driving DCS value through the efficient and effective use of computing assets and driving to the appropriate balance of “doing more with the same” or “doing the same for less” while realizing the value-added capabilities elements of the DCS operating environment.

#### Cross-Tower Coordination

Elements to ensure that all DCS participants: Customers, DIR, the MSI and DCS SCPs are well aligned, communicated, coordinated and supported and are all working within a common operating construct that is as “frictionless” and supportive as possible.

#### Delivery Culture

Increasing capabilities for the State through actively partnering with DCS Customers, prospective Customers and other DCS SCPs and fostering a culture of support, innovation and creativity in enabling the State’s mission.

#### Customer Engagement/Service

Providing service, solutions and support of DCS Customers through active engagement, transparency, innovation and value that DCS provides on State IT challenges.

#### Governance Participation

Participating actively in the STS governance model with DIR, DCS Customers and other SCPs to resolve issues at the lowest level possible and provide customers a voice in decisions that affect them.

#### Business Essentials

Unlocking next generation business models that are currently infrastructure intensive or dependent while providing safe and secure computing essentials that include disaster recovery, business continuity and data loss protection.

#### Driving Legacy Systems Modernization

Using IT infrastructure, platform and cloud assets as logical targets for replacement and modernization of business systems to better serve State constituents (citizens, businesses and State workers).

#### Security and Privacy

Working with Security Operations Services (SOS) SCP and MSI, engineering security and privacy elements into private cloud elements as well as monitoring and tools to help ensure that the State’s risk profile is minimized while ensuring that security/privacy protects State data and systems.

#### Service Order Management

Identifying, enforcing and implementing enterprise standards to drive overall consistency of operations, a unified and simpler operating environment, step changes in systems provisioning and maintenance as well as efficiencies in cost with respect to investment, operating, support and risk models.

#### Talent & Skills

Ensuring that DCS Customers have access to vital skills, experiences, best practices and people that are contemporary/relevant to their needs and include advances in the IT industry.

#### Technology & Automation

Access to better and best practices while removing the human element for error or delay for processes that lend themselves to standardization, automation, templating and tools.

**State of Texas** Department of Information Resources, Data Center Services

#### 1.4.1. Service Support Operating Models and Terminology

- (a) DCS provides many of its services in a variety of operating modes and models as requested by DCS Customers. In general, they should be considered under the following criterion and descriptions:
- (i) **Fully Managed** – Infrastructure, storage, LAN, operating system and security are managed fully. The service element is inclusive of all operations, monitoring, patching, break/fix, updates/upgrades and SLA conventions as applicable to the service element.
  - (ii) **Semi-Managed** – Infrastructure, storage, LAN and security is managed by the Successful Respondent and the operating system is managed by the DCS Customer. In such cases there are clear delineations of responsibility between the DCS Customer and Successful Respondent, and corresponding cost and Service Level considerations.
  - (iii) **Sandbox** –The Successful Respondent shall support provisioning and incident response on as needed basis for DCS Customers allowing these customers a segregated sandbox environment. The DCS Customer retains responsibility for managing most aspects of the service element, and leverages DCS Program elements to enable a sandbox environment. Sandbox support would apply to Public Cloud hosted environments that are essentially self-managed and are not accessible via the DIR Network.
- (b) Additionally, various levels of support/management exist for Backup/Restore and DBMS elements which are presented within the applicable sections of this Exhibit pertaining to those service elements.

#### 1.4.2. Technical Summary: State Public Cloud Environment

##### 1.4.2.1. Configuration Item Summary

There are approximately 900 Public Cloud active configuration items (per DIR’s CMDB) deployed within the DCS Public Cloud environment, over eighty-five percent (85%) of which are on the AWS platform with the remainder on Microsoft Azure. Additional details including hosting site, service tier, and other technical specifics are contained in the Data Room associated with the RFO.

#### 1.4.3. Technical & Operating Summary Objectives: State Public Cloud Business Analytics and Reporting (BAR) Platform

This is a new initiative for DCS in support of DIR’s interest in providing a high-performance platform for Business Analytics and Reporting to DCS Customers. For purposes of establishing a common comparison across all Respondents, DIR is requesting Public Cloud Service offerings that include:

- (i) Configuration of supported open-source distributions of data governance and analytical foundational software based on Hadoop and related enabling software titles;
- (ii) Creation of data governance and protection standards and implementations thereof to protect a DCS Customer’s data in an encrypted form, but allow the “promotion” of these datasets to project zones where agencies can share, combine and perform complex statistical analysis on their data or combine data with other agencies data should they so choose;

- (iii) Provision for future “open data” sharing where the dataset is of public interest and is sanitized as to not include any Restricted data or data elements; and
- (iv) Ongoing operation and maintenance of the Service as well as assistance to DCS Customers in the loading and curation of data within the platform.

## 2. Transition Services

### 2.1. Operations Take Over

At Commencement, the Successful Respondent will take over operations as they exist at that time. The Successful Respondent will be responsible for supporting an orderly and well executed migration/instantiation of supported Public Cloud Services including management and operation, components, documentation and related operational support roles in transitioning from DIR management of cloud providers to the Successful Respondent to enable the Services to be provided.

### 2.2. General Transition Requirements

- (a) The Successful Respondent will be responsible for supporting the migration of supported Public Cloud Service elements in transitioning from DIRs current Service Component Provider (“SCP”) to the Successful Respondent’s Service to enable the Services to be provided as defined within this Exhibit. The Successful Respondent’s responsibilities with respect to Transition Services include the tasks, activities and responsibilities listed below.
- (b) The Successful Respondent shall perform the Transition Services in accordance with the timetable set forth in the Transition Project Plan. Successful Respondent shall assist DIR in connection with DIR's and/or the DCS Customers' evaluation or testing of the deliverables set forth in the Transition Project Plan. Except as otherwise expressly stipulated in the Transition Project Plan (which will appropriately acknowledge that some element of disruption may be inevitable as in any such transition, but shall in all events be minimized), Successful Respondent shall perform the Transition Services in a manner that shall not:
  - (i) disrupt or have an unnecessary adverse impact on the activities or operations of DIR or the DCS Customers,
  - (ii) degrade the Services then being received by DIR or the DCS Customers or
  - (iii) disrupt or interfere with the ability of DIR or the DCS Customers to obtain the full benefit of the Services.
- (c) Without limiting its obligations or responsibilities, prior to undertaking any transition activity, Successful Respondent shall discuss with DIR and the relevant DCS Customers all known DIR and DCS Customer-specific material risks and shall not proceed with such activity until DIR is satisfied with the plans with regard to such risks (provided that, neither Successful Respondent's disclosure of any such risks to DIR, nor DIR's acquiescence in Successful Respondent’s plans, shall operate or be construed as limiting Successful Respondent’s responsibility under this Agreement). Successful Respondent will actively participate in Transition meetings with the MSI and other DCS SCPs.

### 2.3. Knowledge Transfer

- (a) During the period following the Effective Date and prior to the Commencement Date, Successful Respondent will use its best efforts to acquire the practical skill, knowledge and expertise from the personnel who are providing the Services prior to the Effective Date in relation to the delivery of the Services, including the knowledge necessary for the Successful Respondent to perform the Services. Successful Respondent will accomplish such knowledge transfer, as appropriate, by interviewing personnel currently performing the Services as well as reviewing information, records and documents related to the provision of the Services. The information to be reviewed to affect the obligations of such knowledge transfer includes:
- (i) copies of procedures and operations manuals,
  - (ii) relevant system, software, and/or service information,
  - (iii) a list of third-party suppliers of goods and services which are to be transferred to DIR or Successful Respondent,
  - (iv) key support contact details for third party supplier employees, and
  - (v) information regarding work in progress and associated unresolved faults in progress.
- (b) Successful Respondent shall promptly (within one (1) DIR Business Day) notify DIR of any lack of cooperation or assistance on the part of any DCS Customer, DIR Contractor or any third party that impedes or hinders Successful Respondent's efforts to comply with this obligation.
- (i) Transition work includes (at a high level):
  - (ii) Conducting an orderly Transition;
  - (iii) Establishing all Service processes and responsibilities, including on-boarding of all Service Transition and Steady State Service personnel;
  - (iv) Implementing the entire Service inclusive of all DIR required processes, tools, data sharing, and reporting as required by DIR and within the MSI operating model;
  - (v) Ensuring that the Service is performing to DIR requirements and the Successful Respondent is responsible for the Service in its totality with no requirements or obligations residing elsewhere; and
  - (vi) Completing all required deliverables, milestones, and quality standards.

### 2.4. Transition Management Requirements

- (a) During the Transition period, the Successful Respondent will plan, prepare for, and conduct the migration of Service systems operations.
- (b) The Successful Respondent shall:
- (i) Coordinate with DIR to schedule the installation of any required secure connectivity; and
  - (ii) Implement processes and controls to prevent disruption of DCS Customers' business operations, including the interfaces between DCS Customers and various third parties.
  - (iii) Meet with DIR and provide updates as to the status of the work involved in Transition at a time and frequency as mutually agreed to in the Transition Project Plan and upon request by DIR.
  - (iv) Ensure adequate staff are committed to the Transition services across workstreams, including but not limited to one or more dedicated Project Managers.
  - (v) Provide sufficient staff, tools and processes to ensure all Services successfully transition from the incumbent SCP without service degradation to Customers.
  - (vi) Ensure other SCPs successfully transition to Successful Respondent's services by Commencement without service degradation to DCS Customers.
  - (vii) Develop a detailed Transition Plan including the Successful Respondent's approach to transitioning Services from the Incumbent Provider, including if incumbent is currently the DCS Customer. The

- (viii) Transition Plan should include, at a minimum, discovery of all systems, processes, data (e.g., Incumbent ITSM data) and reporting that is required to transition from the Incumbent provider.
- (viii) Provide sufficient staffing to accomplish Transition requirements. These staff must be sufficiently trained on the Successful Respondent's contractual requirements and the Successful Respondent's proposed solution prior to commencing Transition activities.
- (ix) Be responsible for all knowledge transfer from the current provider.
- (x) Provide project management over all Successful Respondent Service Transition and SCP integration Transition.
- (xi) Provide routine reports and communication on Transition status to DIR and SCPs, as directed by DIR.
- (xii) Meet with DIR and SCPs to report on Transition activities, status, issues and risks.
- (xiii) Resolve issues collaboratively with DIR and SCPs in order to meet Transition schedule.
- (xiv) Communicate the status of Transition, training, and changes to DIR.
- (xv) Identify all integration points of the Successful Respondent's solution that require existing SCPs to make changes and notifying each SCP of the required changes at least ninety (90) days prior to Commencement.
- (xvi) Train SCPs as applicable on the Successful Respondent's Services, systems, and SMM processes, focusing on the changes from the incumbent provider.
- (xvii) Create a schedule for all SCPs to complete integration changes and ensure the accuracy of those changes.
- (xviii) Manage the integration of transition tasks and schedule.
- (xix) Test the accuracy of all integration points prior to Commencement.
- (xx) Collaborate with SCPs to resolve any identified issues.

(c) DIR, other DCS SCPs, and/or the MSI will:

- (i) Obtain and provide current information, data, and documentation related to the Transition (e.g., Third Party suppliers, Successful Respondent information, facility data, inventory data, existing operational processes and procedures, systems documentation and data, configuration documentation and data), decisions and approvals, within the agreed time periods to the extent it is available and non-proprietary;
- (ii) Establish secure network connections as necessary;
- (iii) Assist the Successful Respondent in identifying, addressing, and resolving deviations from the Transition Plan and any business and technical issues that may impact the Transition; and
- (iv) Develop the Transition meeting schedule (i.e., planning, review, and status) with the Successful Respondent and applicable SCPs, including the frequency and location, and attend such meetings in accordance with the established schedule.

## 2.5. Transition Project Plan

Respondent shall include a preliminary Transition Project Plan as part of its Response. After Contract Execution, the Successful Respondent will deliver an updated Transition Plan as a Critical Deliverable.

### 2.5.1. Transition Project Plan Proposal Requirements

(a) DIR encourages Respondents to demonstrate a thorough understanding of the nature of the work and Successful Respondent responsibilities. To this end, the Respondent must submit a Transition Project Plan (as part of their proposal) that the Successful Respondent will use to create a consistent and coherent Transition management plan. The Transition Project Plan should include detail sufficient to give DIR an understanding of how the Respondent's knowledge and approach will:

- (i) Manage the Project;
- (ii) Guide Project execution;
- (iii) Document planning assumptions and decisions;
- (iv) Work with the MSI to integrate into the MSI's systems.
- (v) Facilitate communication among stakeholders;
- (vi) Define key management review as to content, scope, and schedule; and
- (vii) Provide a baseline for progress measurement and Project control.

**State of Texas** Department of Information Resources, Data Center Services

- (b) At a minimum, the Respondent's Project Plan must include the following:
- (i) Work breakdown structure;
  - (ii) High-level Project schedule for all Project Deliverables and milestones;
  - (iii) Who is assigned responsibility for each Deliverable within the work breakdown structure to the level at which control will be exercised;
  - (iv) Performance measurement baselines for technical scope and schedule;
  - (v) Major milestones and target date(s) for each milestone that are consistent with this RFO's dates;
  - (vi) Description of the Respondent's proposed organization(s) and management structure responsible for fulfilling the Contract's requirements and delivering the Work, in terms of oversight and control;
  - (vii) Definition of the review processes and reviewers (e.g., MSI, DIR, or DCS Customer as applicable) for each milestone and Deliverable (e.g., mandatory design review) and a description of how the parties will conduct communication and status review;
  - (viii) Description of the Project issue resolution process including an escalation plan, where the escalation plan includes contact information for each person identified in the proposed problem reporting and escalation procedure and describes the amount of time elapsed before a problem is escalated within their organization;
  - (ix) Description, plan, and schedule of how the Respondent plans to ensure consistent, regular communications with DIR regarding the status of the Transition activities;
  - (x) Description of how Respondent plans to ensure Project Management best practices are to be utilized and followed for the Transition, across one or more assigned Project Managers and any additional Project Management Office support staff;
  - (xi) If the Respondent chooses to use subcontractors, this part of the Respondent's Proposal must describe its approach to using and managing its subcontractors (should any be used) effectively.
- (c) The Respondent's Project Plan will be scored as part of the evaluation of offers.

#### 2.5.2. Transition Project Plan Critical Deliverable

- (a) The Successful Respondent must submit and present to DIR a detailed Transition Project Plan for review, feedback, and approval on or before the date set forth in **Attachment 1.1 Deliverables**. The Transition Project Plan must include all phases of the transition for which the Successful Respondent has responsibility, including Deliverables and tasks as well as any tasks and dependencies that may be outside of the Successful Respondent's responsibility but may influence or relate to the Successful Respondent's work and ability to complete work as planned. In addition to maintaining steady-state operational capability, the Successful Respondent shall include any identified security concerns that will be addressed during Transition or any agreed upon Transformation Projects. If the Transition Project Plan submitted by the Successful Respondent is not acceptable to DIR, Successful Respondent shall address and resolve any questions or concerns DIR may have and promptly incorporate any modifications, additions, or deletions requested by DIR. The Successful Respondent shall revise and resubmit the Transition Project Plan until accepted in writing by DIR. Upon DIR's acceptance, the Transition Project Plan shall automatically be incorporated into this Agreement by reference and shall supersede and replace all prior Transition Project Plans.
- (b) The Transition Project Plan must include a detailed task/activity level for the planned Transition period, inclusive of activities and named resources engaged by the Successful Respondent and all roles with effort hours required for DIR and/or current SCP(s). The Transition Project Plan must also propose for DIR consideration, a proposed schedule of regular status meetings with DIR to ensure DIR remains informed on the status of all Transition activities. DIR may also request additional status updates outside of the regularly scheduled meetings at their discretion. The Transition Project Plan must be maintained by the Successful Respondent on an ongoing basis through Transition and made available on a DIR-provided document collaboration site to all DCS stakeholders associated with the Transition of the Service. Following acceptance

of the Transition Project Plan deliverable, further changes to the plan shall be incorporated as mutually agreed to by the Parties.

- (c) The Transition Project Plan must include an updated Staffing Plan (for the Successful Respondent's resources and MSI, SCPs, and DIR resources that are required to participate in the work including Successful Respondent-related activities). The Staffing Plan must include the number of resources by role for the high-level tasks.
- (d) After submission of the Critical Deliverable referenced in **Attachment 1.1 Deliverables**, the Successful Respondent must update the Detailed Transition Plan monthly, ensuring that the level of specificity of the plan for a rolling six (6) month period is defined to the task and named resource level. Given the anticipated multi-month, multi-phase nature of this project, ensure that time periods beyond this six (6) month period are accurately portrayed and forecast based on the actual project performance to date and anticipated (or realized) downstream impacts to subsequent phases and activities (if applicable). As an example, the initial project plan will include details for the first six (6) months and activity/milestone level (sufficient to track the overall progress of the program) for the anticipated remainder of the transition based on the current understanding of project scope and phasing.
- (e) DIR will:
  - (i) Cooperate with the Successful Respondent to assist and support with the completion of the Transition as DIR finds necessary;
  - (ii) Assist the Successful Respondent in managing SCP facing efforts and cooperation with agreed Successful Respondent created roles, responsibilities, plans and requirements; and
  - (iii) Approve or reject the completion of each phase of the Transition Plan in accordance with the acceptance criteria after written notice from the Successful Respondent that it considers such phase complete.
  - (iv) Work with the Successful Respondent during negotiations to document and define the acceptance criteria and appropriate number of business days necessary for such reviews. Should DIR reject the Plan or associated Deliverables in part or in full, the Successful Respondent must, at no additional cost, correct all deficiencies and resubmit for DIR's review until DIR accepts the Deliverable. Should the Successful Respondent determine DIR's review of Deliverables or Work Products will impact the Successful Respondent's ability to execute the Transition in accordance with the agreed and established Project Plan, the Successful Respondent must notify DIR promptly with a request for expedited review of Deliverables or Work Products. In no case must an expedited review be requested under circumstances that are within the Successful Respondent's direct control or as they relate to Deliverables deemed deficient by DIR.

### 2.5.3.Kickoff

The Successful Respondent, in conjunction with DIR staff, the MSI, and other impacted DCS SCPs, must plan and conduct a Project kickoff meeting presentation to the sponsors, key stakeholders, and core project team after the mobilization effort. At a minimum, the presentation must include a high-level overview of the following:

- (i) Project scope and schedule;
- (ii) Goals of the Project;
- (iii) Communications and regular meetings;
- (iv) Methodology, approach, and tools to achieve the goals;
- (v) Roles, responsibilities, and team expectations;
- (vi) Tasks, Deliverables, and significant Work Products; and
- (vii) Risk, issue, resolution, and milestone reporting.

#### 2.5.4.Meeting Attendance and Reporting Requirements

- (a) The Successful Respondent's project management approach must align with the established Project Management processes documented in the SMM and adhere to the following meeting and reporting requirements, unless otherwise agreed to by DIR:
- (i) Immediate Reporting - The Project Manager or a designee must immediately report any Project staffing changes to DIR's Project Manager in accordance with Article [5 Successful Respondent Personnel Requirements](#)
  - (ii) Attend Weekly Status Meetings - The Successful Respondent's Project Manager and applicable Project team members must attend weekly status meetings with DIR's Project Manager and applicable members of the DIR Project team as necessary to discuss Project issues. These weekly meetings must follow an agreed upon agenda which is distributed by the Successful Respondent no later than forty-eight (48) hours before the meeting and allow the Successful Respondent and DIR to discuss any issues that concern them.
  - (iii) Provide Weekly Status Reports - The Successful Respondent must provide written status reports to DIR's Project Manager at least one (1) full Business Day before each weekly status meeting. At a minimum, weekly status reports must contain the items identified below:
    - A. Updated Transition Project Plan files on electronic media acceptable to DIR;
    - B. Status of currently planned tasks - specifically, identifying tasks not on schedule and a resolution plan to return to the planned schedule;
    - C. Issues encountered, proposed resolutions and actual resolutions;
    - D. The results of any tests;
    - E. A Problem Tracking Report must be attached;
    - F. Anticipated tasks to be completed in the next week;
    - G. Task and Deliverable status, with percentage of completion and time ahead or behind schedule for tasks and milestones;
    - H. Proposed changes to the Project work breakdown structure and Project schedule, if any;
    - I. Identification of Successful Respondent staff assigned to specific activities;
    - J. Planned absence of Successful Respondent staff and the expected return date;
    - K. Modification of any known staffing changes; and
    - L. System integration/interface activities.
  - (iv) Prepare and Lead Monthly Status Reports – During the Project, the Successful Respondent must submit a written monthly status report to DIR's Project Manager by the fifth (5th) Business Day following the end of each month. At a minimum, monthly status reports must contain the following:
    - A. A description of the overall completion status of the Project in terms of the approved Transition Project Plan (schedule and cost, if applicable);
    - B. Updated Project work breakdown structure and Project schedule;
    - C. The plans for activities scheduled for the next month;
    - D. The status of all Deliverables, with percentage of completion;
    - E. Time ahead or behind schedule for applicable tasks;
    - F. A risk analysis of actual and perceived problems, including recommended remediations and a red, yellow green status indicator;
    - G. Testing status and test results; and
    - H. Strategic changes to the Transition Project Plan, if any.
- (b) The Successful Respondent's proposed format and level of detail for the status report is subject to DIR's approval.

### 2.5.5. Transition Documentation and Collaboration

The Successful Respondent must use the MSI Portal for document management and team collaboration. This hosted document management and team collaboration capability provides access through internal state networks and secure external connections to all project team members, approved project stakeholders, and participants. In conjunction with the utilization of this tool, the Successful Respondent must:

- (i) Structure the document management and collaboration pages and data structures in such a manner as to deliver on the overall requirements of the Project; and
- (ii) Load all Service-related documentation, deliverables, reference material and/or configuration documentation onto the MSI's document collaboration tool. The Successful Respondent must confirm with the MSI that all documentation has been provided and is readily available.

### 2.5.6. Determination of Responsibility (Successful Respondent and Other State Vendors)

The Successful Respondent shall be responsible for:

- (i) Failures that are exclusively in the Successful Respondent's area of responsibility, or that are exclusively staffed or performed by Successful Respondent-provided personnel;
- (ii) Failures where DCS personnel (MSI, SCP, or DIR) are following established Successful Respondent processes where, as a result of issues, defects, omissions, or inconsistencies in these designed and provided processes are shown to be the primary source of the failure;
- (iii) Failures where DCS Services personnel (MSI, SCP, or DIR) are not provided processes that are the Successful Respondent's responsibility to design, develop, implement, or document;
- (iv) Failures where Successful Respondent Services personnel has an exclusive role or responsibility and is not dependent on DIR resources to complete the tasks associated with the failure;
- (v) Failures arising where DCS Services Personnel (MSI, SCP, or DIR) are following the direction of a Successful Respondent resource where that direction is inconsistent with established policies and procedures;
- (vi) Failures arising where a DCS resource is performing a role, responsibility, or task that is outside of the established DCS providers' responsibility but within the Successful Respondent's responsibility area on an ad hoc or temporary basis in lieu of a Successful Respondent resource at the request of the Successful Respondent;
- (vii) Any failure arising from Successful Respondent personnel not following established State security, privacy, or other IT policies;
- (viii) Any failure resulting from a subcontractor working for, or at the direction of the Successful Respondent; and,
- (ix) Failures arising from Successful Respondent-owned equipment or computing devices coincident with providing the in-scope services.

### 2.5.7. Organizational Change Management

During Transition, the Successful Respondent will be required to document all functions and technologies of the organization.

The Successful Respondent will be responsible for implementing and training all stakeholders on the following, which should be documented in the Service Management Manual (SMM):

- (i) Service Operational Processes and Procedures;
- (ii) DIR Operations Service Team Change Management and Training; and
- (iii) DCS Customer-, MSI-, or DCS SCP- facing equipment, tools, and processes required to satisfy the business, functional, and technical requirements.

### 2.5.8. Operational Readiness

The Successful Respondent will assess its readiness to assume operations and maintain the functionality deployed under this Exhibit. The Successful Respondent will recommend strategies as required to ensure DIR, DCS Customers and DCS SCPs are prepared to support any new system functionality. The Successful Respondent will design the Service as to ensure that the following required MSI reports, data requirements, and integrations are developed and completed as necessary to operate the Service in the DIR environment:

- (i) Confirmation of integration with MSI and other SCPs as required;
- (ii) Confirmation of alignment with MSI processes/procedures in the SMMs and identification of any critical gaps in documentation or processes;
- (iii) Updated Key Personnel contact information and staff employment status;
- (iv) Documented Solution Designs, Reference Architectures, Standards, and Service Descriptions
- (v) Documented operational processes/procedures needed to deliver Services and status of publication on the MSI portal;
- (vi) Status of Software license transfers;
- (vii) Status of hardware transfers;
- (viii) Status of lease transfers;
- (ix) Billing process including detail for invoices;
- (x) Status of operating agreements between the Successful Respondent and the MSI and Service Component Providers (SCPs); and
- (xi) Knowledge transfer programs.

### 2.5.9. Staffing Plan and Time Commitment

(a) The Successful Respondent shall provide a summary of full time equivalent (FTE) personnel needed for transition of the Services along with Service design and implementation. Additionally, any requirements of DIR, DCS Customers, MSI, or of the SCP(s) performing the current service, as well as delivery and space planning considerations, will be outlined in the table:

**Table 2: Full Time Equivalent (FTE) Personnel**

Successful Respondent Proposed Role(s)	% of FTE Time Spent at DIR ADC Work Location	% of FTE Time Spent at DIR SDC Work Location	% of FTE Time Spent at Respondent Work Location	Engagement Period
<b>Respondent Transition Team and Roles</b>				
Successful Respondent Account Representative	60%	20%	20%	Transition Period XX/2019 – YY/2019
Operations Service Lead	100%			Transition Period XX/2019 – YY/2019
Security Systems Lead	100%			Transition Period XX/2019 – YY/2019
Operating Systems Lead	100%			Transition Period XX/2019 – YY/2019
Storage / Backup Systems Lead	80%	20%		Transition Period XX/2019 – YY/2019
Virtualization Engineer	100%			Transition Period XX/2019 – YY/2019
Cloud Technical Architect(s)	50%	20%	30%	Transition Period XX/2019 – YY/2019
Cloud Solutions Architect(s)	50%	20%	30%	Transition Period XX/2019 – YY/2019
Cloud Portfolio Architect	25%		25%	Transition Period XX/2019 – YY/2019

Successful Respondent Proposed Role(s)	% of FTE Time Spent at DIR ADC Work Location	% of FTE Time Spent at DIR SDC Work Location	% of FTE Time Spent at Respondent Work Location	Engagement Period
Performance and Capacity Engineer	Periodic, 10%		Periodic, 20%	Transition Period XX/2019 – YY/2019
Cloud Engineer	50%		50%	
Level 2 Administrator (4) – Onsite	100%			Transition Period XX/2019 – YY/2019
Level 3 Administrator (3) – Remote			50%	Transition Period XX/2019 – YY/2019
Production Change Manager			100%	Transition Period XX/2019 – YY/2019
<i>add/modify rows as required</i>				
TRANSITION ROLES Requested from DIR or Incumbent Service Component Provider (SCP)				
Transition Executive	100%		-	XX/2019 – YY/2019
Transition Managers (Server, Security) (3)	100%		-	XX/2019 – YY/2019
Functional SME (10)	80%		20%	XX/2019 – YY/2019
MSI Service Management SME				XX/2019 – YY/2019
Finance/Admin SME				XX/2019 – YY/2019
<i>add/modify rows as required</i>				

**NOTE:** The values in this **sample table 2** above are for illustration purposes only. Respondents should remove these illustrative artifacts and populate the table based on their proposed team and work locations. Respondent may add additional rows as necessary.

- (b) FTE time shall represent those hours in direct support of the Service. In some cases, this number may be less than 100%.

#### 2.5.10. Remedies for Transition Failure

- (a) In the event that Successful Respondent fails to identify and resolve any problems that may impede or delay the timely completion of each task in the Transition Plan, without prejudice to DIR's other rights and remedies under the Agreement or at law or equity,
- (i) Successful Respondent will provide, at its sole cost and expense, all such additional resources as are necessary to identify and resolve any problems that may impede or delay the timely completion of each task in the Transition Plan, and
  - (ii) DIR may equitably reduce the Charges set forth in **Exhibit 2 Pricing** in an amount estimated by DIR to account for the Services that DIR and/or the DCS Customers are not receiving or did not receive, and
  - (iii) DIR may suspend or delay the performance of the Transition Services and/or the transition of all or any part of the Services, including the Commencement Date.
- (b) Successful Respondent represents and warrants to DIR that, as of the Commencement Date, it is ready to commence performing the Services in accordance with the terms of this Agreement, including with respect to pricing, applicable Service Levels, and other performance obligations. In the event that such representation and warranty is not true and correct, Successful Respondent will reimburse DIR for any costs or expenses incurred by DIR as a result of the failure of such representation and warranty to be true and correct. In the event that Successful Respondent is required to perform any Transition activities following the Effective Date, Successful Respondent will complete such activities at its own cost and expense and in such a manner so as to not materially disrupt or cause any material adverse impact on DIR's operations or activities unless otherwise agreed to with DIR.

### 3. Steady State Operations and Support Services

- (a) DIR's requirements with respect to the support, monitoring, maintenance, middleware, database management, security services, as well as Public Cloud Services evolution as part of steady state (e.g., "day-to-day operations") will pertain to the period from the Commencement Date to the completion of the contracted period. The Successful Respondent will, through ongoing support and maintenance control processes, support the current implementation as well as solutions developed by the Successful Respondent during the term of the Contract.
- (b) The Successful Respondent shall support DIR in evaluating, making recommendations, selecting, and onboarding new cloud providers, negotiating contracts, managing renewals, handling contract disputes with cloud providers, and evaluating and selecting value added services and products that complement the cloud provider offerings (e.g., cloud provider marketplace offerings). The Successful Respondent shall provide and perform governance activities across all cloud providers, to ensure ongoing alignment to DCS Customer demand, DCS Customer regulatory compliance, and adherence to data and privacy standards, across all Public Cloud providers. Finally, the Successful Respondent shall provide Business Analytics and Reporting (BAR) by leveraging Public Cloud provider capabilities to allow DCS Customers to unlock the potential in the data residing in State IT systems. BAR is an optional project but DIR is requesting the Respondent include in their proposal a Public Cloud design to meet the requirements as defined in Section 7.3.3 Project 1: Business Analytics and Reporting (BAR) Platform Service Requirements of this document.
- (c) Steady State Services includes activities to support DIR's in-scope Public Cloud environment, workloads, processes, and systems management roles and responsibilities for the Public Cloud environment. Steady State Services include responsibilities and activities to support Public Cloud products and corresponding workloads within virtual networks, operating system instances, processes, and systems management roles services for IaaS, PaaS, SaaS, virtual private containers, microservices, deployment slots, container technologies, Serverless architectures and Application hosting services. Responsibilities for the DCS environment include integration with other DCS SCPs to ensure availability of Services.

#### 3.1. General Requirements

DIR has designed its operating model to leverage a Multi-Sourcing Integrator (MSI) which operates on an ITIL-based platform with specific tools and processes that all DCS service providers will utilize. Requirements related to these cross-functional processes and components are detailed in Article 9 of this Exhibit.

##### 3.1.1. Cloud Service Tiers

The DCS Service must offer the following service tiers to DCS Customers. The following table summarizes the required tier structure, and general scope of services for each. The Successful Respondent shall deliver these different service tiers and the monitoring or support for each category below as described in the technical response and detailed in the SMM. All Strategy Management functions listed below will be performed in support of and under leadership of TSS SCP.

**Table 3 – Cloud Service Tiers**

Service Tier	Sandbox	IaaS	IaaS	IaaS	PaaS	SaaS
<b>Strategy Management</b>	Development	Non-Std	Semi-Managed	Fully Managed	Fully Managed	Configuration Management
Market Expertise	Yes	Yes	Yes	Yes	Yes	Yes
Enterprise Roadmaps	Yes, by PCM under TSS	No	Yes, by PCM under TSS			
Product and Service Evaluation	Yes, by PCM under TSS	No	Yes, by PCM under TSS			
Service Catalog Management	Yes, by PCM under TSS	No	Yes, by PCM under TSS			
Proof of Concepts	Yes, by PCM under TSS	No	Yes, by PCM under TSS	Yes, by PCM under TSS	Yes, by PCM under TSS	n/a
Detailed Cloud Assessments	Yes, by PCM under TSS	No	Yes, by PCM under TSS	Yes, by PCM under TSS	Yes, by PCM under TSS	n/a
Request for Solution	Yes	Yes, into In New Environment	Yes	Yes	Yes	n/a
Technology Planning	Yes	No	Yes	Yes	Yes	n/a
<b>Monitoring &amp; Administration</b>	Development	Non-Std	Semi-Managed	Fully Managed	Fully Managed	Configuration Management
Broker	No	No	Yes	Yes	Yes	n/a
Provision	No	Yes	Yes	Yes	Yes	n/a
Physical Network	No	n/a	n/a	n/a	n/a	n/a
Virtual Network	No	Optional	Yes	Yes	Yes	n/a
Storage	No	n/a	n/a	n/a	n/a	n/a
Virtualization	No	n/a	n/a	n/a	n/a	n/a
OS	No	No	No	Yes	n/a	n/a
Middleware	No	No	No	Optional	Optional	n/a
DBMS	No	No	No	Optional	Optional	n/a
Backup	No	No	No	Yes	Yes	n/a
DR Planning	No	No	Yes	Yes	Yes	n/a
DR Testing & Execution	No	No	No	Optional	Optional	n/a
Applications	No	No	No	Optional	Optional	n/a
Security	No	Yes	Yes	Yes	Yes	n/a
PCP Service Mgt & Escalations	Yes	No	Yes	Yes	Yes	Yes
<b>Configuration Management</b>	Development	Non-Std	Semi-Managed	Fully Managed	Fully Managed	Configuration Management
Physical Network	No	n/a	n/a	n/a	n/a	n/a
Virtual Network	No	Yes	Yes	Yes	Yes	n/a
Storage	No	Yes	Yes	Yes	n/a	n/a
Virtualization	No	Yes	Yes	Yes	n/a	n/a
OS	No	No	No	Yes	n/a	n/a
Middleware	No	No	No	Optional	Optional	n/a
DBMS	No	No	No	Optional	Optional	n/a
Backup	No	No	No	Yes	Yes	n/a
Disaster Recovery	No	No	No	Yes	Yes	n/a
Applications	No	No	No	Yes	Yes	n/a
Security	No	Optional	Yes	Yes	Yes	n/a
<b>Service Management</b>	Development	Non-Std	Semi-Managed	Fully Managed	Fully Managed	Configuration Management
Hours of Coverage	24x7	9x5	24x7	24x7	24x7	24x7
Incident Response	Yes	Yes	Yes	Yes	Yes	Yes
Availability Measurement	No	No	OS	OS	Platform	Varies based on Service

### 3.1.2.DCS Impact and Urgency Definitions

The DCS impact and urgency definitions are documented in the SMM.

### 3.1.3.Technology Planning

The Successful Respondent will participate with the TSS and MSI in the development of a multi-year Service roadmap inclusive of all projects, optimization and transformation initiatives as defined in Section 4, Steady State Service Evolution.

### 3.1.4. Customer Enablement

One of the goals of the NextGen DCS program for Public Cloud is to allow Customers to consume services in the Public Cloud as natively as possible with technical, delivery and security assurances while not limiting the ability to leverage the ever-evolving landscape of Public Cloud Services. The Successful Respondent will:

- (i) Provide the ability to provision and support services in alignment with Public Cloud capabilities.
- (ii) Enable Customer self-provisioning capabilities consistent with program standards, reference architecture and security policies, including service operations (e.g. asset management, reporting, billing, service level management, etc...).
- (iii) Provide ability to integrate with MSI service catalog.
- (iv) Provide ability for access controls to services and operational functions based on defined Customer and Successful Respondent support responsibilities.
- (v) Provide ability to integrate with Cloud Service Provider native console and / or service catalogs, including:
  - A. Operational access for logs, diagnostics, analysis, service starts and stops, etc...
  - B. Provisioning access to allow fulfillment of provision requests based on templates aligned to DIR standards and policies and/or application tools available from CSP
  - C. Enable deployment of the templated cloud infrastructure with role-based security and automated fulfillment leveraging Public Cloud best practices delivered with the MSI Service Catalog integration.
    - 1. Role based security will be delivered based upon Customer requirements and will be delivered within defined DIR policies and governed by the principle of “least privilege” required to effectively balance Customer requirements with program goals.

## 3.2. DCS Public Cloud Center of Excellence (CoE)

### 3.2.1.Public Cloud Center of Excellence Foundational Concepts

- (a) The Successful Respondent will collaborate with DIR and TSS and utilize industry and other best practices to design and establish a Public Cloud Center of Excellence (CoE) for DIR as follows:
  - (i) Support the establishment of a DIR-led group that comes together to discuss and collaborate on large-scale concepts, granular ideas, tools, and solutions pertaining to a specific platform or business initiatives;
  - (ii) Assist DIR in development and implementation of a mission, charter statement and operating protocols that focus on creating, developing, and promoting proven practices and ideas that will

- help streamline processes across Public Cloud development projects Statewide and improve the quality of both worker and customer experiences;
  - (iii) In conjunction with TSS and DIR, establish a development support network to share experiences, standards and procedures that result in reusable, high quality and repeatable implementation (or implementation elements) for common use across the Public Cloud wherever possible.
  - (iv) Support TSS in establishing standardized reference architectures, security policies, and automated build configurations highly leveraging native cloud provider capabilities which are closely aligned to customer use case demand.
  - (v) Articulate methods, techniques, and disciplines that clearly articulate how service evolution of Public Cloud capabilities and its impact on current and potential DCS Customers will be managed to enable continued value is achieved across the DCS program.
  - (vi) Provide continued visibility and focus on reducing complexity, stream-lining processes, and automating tasks.
- (b) As part of the work, the Successful Respondent will establish membership criterion, meeting cadence and agenda, discussion topics, inclusion of DIR and non-DIR speakers (e.g., success stories, “better practices,” roadmaps, and general awareness elements). This CoE will work in conjunction with the TSS SCP to deliver solution services and ensure consistency of strategy and lifecycle services are managed across the environment.

### 3.2.2. Establish Standards and Best Practices

- (a) Given the scope, breadth, and velocity of Public Cloud-based development projects, it is essential to adopt a platform approach to Cloud projects where development strategies, methodologies, design factors, integration methods, reports and conversions are shared across the DCS enterprise to the greatest extent possible as to minimize cost, development risk and maximize quality and inevitably the outcomes associated with DCS Customer Public Cloud projects. These practices must be developed in conjunction the MSI to ensure alignment with Demand and Service Management procedures.
- (b) As part of the work, the Successful Respondent will create DCS Best Practices, including (at a minimum):
- (i) In coordination with the MSI and Private Cloud SCP, develop strategies, architectures, products and process flows for supporting cross-platform (e.g., Public-to-Private, Public-to-Public) service management capabilities (e.g., provisioning, component management, reporting).
  - (ii) Environment Management Best Practices - A reference document to establish best practices for environments, including establishing environments, managing environments, and environment refresh processes.
  - (iii) Enterprise Public Cloud Collaboration - A reference document and creating of services to establish standard methods by which the project team can collaborate with their various DIR support teams and providers, as well as any other relevant project teams.
  - (iv) Solution Accelerator Library - a reference of projects and their existing capabilities that can be used to build solutions.
  - (v) Shared Solution Development (e.g., User Provisioning, Deployment) - Solutions developed for the greater good of DIR’s Public Cloud platform.
  - (vi) Promote consistency through automation of service operations by examining frequency of requests, commonalities between products, services and applications and streamlining process.
  - (vii) Support MSI with optimization of Customer experience using Service Catalog through leveraging Public Cloud best practices, particularly around automation and orchestration.

### 3.2.3.DevOps Support and Development Accelerators

DIR seeks to assist DCS Customers in developing applications across the full spectrum of the Public Cloud Services that balance portability, scalability, and capability. DIR and DCS Customers are moving to a more agile approach to deploying applications in the Public Cloud, by leveraging DevOps principles and practices. The Successful Respondent must provide development accelerator capabilities that address the following (as examples):

- (i) Technologies and tooling services that support automated, rapid and incremental end-to-end development and deployment of applications (e.g. SDLC pipelines);
- (ii) Application Programming Interfaces (APIs) that are capable of creating, reading, updating, and deleting Cloud Provider resources, and that are complementary to the MSI cloud management capabilities (as described in MSI Exhibit 2.1 v1.14);
- (iii) IaaS/PaaS solutions that support DCS Customer ability to setup development environments that mirror production, enable application portability, and on-demand access; and
- (iv) Continuous deployment of new services and capabilities in an agile manner based on evolution of cloud provider services and capabilities.

### 3.2.4.Solution Governance

The Successful Respondent will be responsible for supporting a governance framework across the Public Cloud Service to ensure alignment to customer demand, regulatory compliance, data and privacy standards (e.g., PII) are in place and enforced, and to conduct recurring audits of DCS Customer solutions across all Public Cloud providers.

### 3.2.5.User Group Sessions

The Successful Respondent will support DIR in the visioning and establishment of a Public Cloud user group and function as an active participant in the Public Cloud user group's creation and ongoing meetings. As part of the work the Successful Respondent will:

- (i) Work with the group to establish a monthly agenda;
- (ii) Encourage participation and collaboration among DIR, DCS Customer, DCS Prospects, and other DCS Stakeholders;
- (iii) Identify within DIR (e.g., project teams and leaders) and outside of DIR (Public Cloud providers and other industry leaders) speakers, relevant topics for user group meetings and presentations; and
- (iv) Use sessions to promote sharing, assistance, standards, reference architectures, policy, and high quality / high value Public Cloud projects – for those projects that lend themselves to Public Cloud deployments – in such a manner as to reduce implementation risk and cost and increase outcomes in high quality systems for DIR.
- (v) Assist DIR and MSI in development of a Public Cloud training regimen designed to assist DCS Customers (within the budgets and priorities of individual agencies) in developing “awareness”, basic skills, proficiency and expertise in Public Cloud development and management practices.
- (vi) Work with DCS Customers and DCS Prospects for training needs based on their actual or committed Public Cloud project and operations profile;
- (vii) Develop and maintain partnerships with Public Cloud Providers and, utilizing these relationships, foster collaboration between DCS Customers and Public Cloud Providers.

### 3.3. Procurement Management

#### 3.3.1. Software as a Service (SaaS) / Platform as a Service (PaaS) Purchases on Behalf of Customer

- (a) In addition to Customers purchasing PaaS through the PCM from DCS Public Cloud Providers, the Successful Respondent shall provide as part of their service catalog, the option for Customers to purchase SaaS and PaaS (including Business Process as a Service (BPaaS) or any X as a Service (XaaS) that fits within the general scope of the award) from Public Cloud providers not currently approved by DIR. In such cases as the purchase is from a non-DIR approved provider, a DCS Program exemption as well as technology and security validation shall be required to be completed by Successful Respondent.
- (b) The Successful Respondent shall ensure the most cost-effective decisions are made to provide business value for DCS Customers, which may include engaging with vendor or TSS to verify the Customer's requested SaaS purchase meets the technical definition of Software as a Service or Platform as a Service.
- (c) These purchases are invoiced to Customers as Software as a Service Charges (SaaS) as defined in **Exhibit 2 Pricing**. These requests include:
  - (i) Initial purchase – These purchases shall be made in the name of the Customer and are invoiced to the Customer at the Successful Respondent's purchase price.
  - (ii) Subscription Renewals – Renewals for subscriptions are invoiced to the Customer at the Successful Respondent's purchase price as SaaS.
- (d) Successful Respondent shall also engage DCS customers as required prior to and during any negotiations of terms and conditions and obtain written approval from the DCS Customer for the product's terms and conditions. All purchase contracts must be assignable to DIR or the DCS Customer at termination. The Successful Respondent is responsible for tracking all subscriptions and initiating renewals with the customer.
- (e) In connection with the foregoing, the following subsections shall apply.

##### 3.3.1.1. Purchases under DIR Master Agreements

If the requested is available under DIR master agreements between DIR and the third-party vendor, Successful Respondent shall use these master agreements to procure unless Successful Respondent can procure such at a lower cost than such can be procured through such master agreements. Successful Respondent shall provide reasonable documentation respecting the foregoing as may be requested by DIR. Purchasing process details are maintained in the SMM. The Successful Respondent shall also:

- (i) Support DIR in XaaS negotiations to achieve the best value for the State;
- (ii) Through defined Successful Respondent quarterly business reviews across various customers, the Successful Respondent will make reasonable efforts to help identify cost reduction and value opportunities for DIR and DCS Customers.

### 3.3.1.2. Successful Respondent Agreements

Successful Respondent may use agreements between Successful Respondent and third-party vendors if permitted by such agreements to procure products and services on DIR's or a DCS Customer's behalf. Successful Respondent's use of such agreements shall be conditioned on and subject to the following:

- (i) DIR or the DCS Customer approving in advance the terms, conditions and pricing of such agreements and any financial or other commitments made therein by or on behalf of DIR or the DCS Customers;
- (ii) Where permitted by such agreements and consistent with DIR's approval, Successful Respondent passing through to DIR any refunds, credits, discounts or other rebates to the extent such amounts are directly allocable to DIR;
- (iii) Such agreements offering more favorable pricing and equivalent or better terms and conditions for the requested product or service than the master agreements between DIR and third party vendors;
- (iv) Giving DIR and the DCS Customers price quotations and other benefits consistent with Successful Respondent's favorable third party vendor arrangements where permitted by such vendors;
- (v) To the extent reasonably practicable, using the aggregate volume of Successful Respondent's procurements on behalf of itself, DIR, the DCS Customers and other customers to obtain more favorable pricing and equivalent or better terms and conditions for the requested product or service; and
- (vi) After evaluation of DIR co-operative contracts and verification that such contracts do not offer greater business value for DCS customers.

### 3.3.1.3. Volume Discount Pricing

- (a) One of the goals of the DCS program is to aggregate volume across customers to obtain more favorable pricing for the enterprise. For those SaaS products requested by multiple customers, the Successful Respondent shall attempt to obtain volume discount pricing.
- (b) Successful Respondent shall negotiate volume discount pricing with third party vendors to achieve the most favorable rates for DCS Customers.

## 3.4. Operations and Monitoring

The Successful Respondent must provide operations support services for all in-scope environments and services for IaaS, PaaS, SaaS, virtual networks (e.g. VPC), Microservices, Serverless architectures and Application hosting services, including, but not limited to:

- (i) Install, configure and provide ongoing support of software and monitoring and reporting tools and services.
- (ii) Perform all measurement and reporting for Public Cloud hosted platforms as required to support services as defined in Section 6, Performance model and Service Level Agreements
- (iii) Monitoring, including real time mechanisms for monitoring systems, including: availability, auto-scaling, performance, capacity and overall environment health as defined in the SMM and required to support SLAs as defined in Section 6 Performance Model and Service Level Agreements

- (iv) Deploy URL monitors to test SaaS platform availability from each of the cloud regions as well as ADC and SDC, and collaborate with Customers that leverage SaaS platforms to place a monitor that will be representative of the Customer access method to the SaaS Platform.
- (v) Integrate Monitoring with the MSI ITSM platforms to allow electronic event and incident management integration and provide for real-time systematic notification of performance issues and any events.
- (vi) Conduct 7x24x365 monitoring, event management and service restoration activities of Public Cloud platforms including real-time monitoring and reporting of capacity, stability, and performance of Services, Software and Platforms.
- (vii) Provide full monitoring integration with MSI and SCP operational support processes (e.g., SIEM, Incident Management, Change Management, Asset and Inventory Management, etc.).
- (viii) Establishment and monitoring of proactive alarms in accordance with thresholds defined in the SMM.
- (ix) Provide end-to-end visibility to MSI and DIR-approved Users or DCS Customers to view performance statistics (real-time and historical) on Public Cloud platforms.
- (x) Coordinate with the business partners, Third Party Vendors, other SCPs, DIR, and DCS Customers as appropriate on projects to install/upgrade hardware and software.
- (xi) Provide status and trending reports as required, including:
  - A. reports to highlight incidents and problems and establish predetermined action and escalation procedures when batch window incidents and problems are encountered.
  - B. report to DIR and DCS Customers on resource shortages, and report utilization statistics and trends to DIR and DCS Customers on a monthly basis at a level of detail sufficient to identify exceptions.
- (xii) Actively support DCS Customer and SCP production staff to create and adapt IT operational processes and procedures related to the in-scope environments and standards;
- (xiii) Assume the responsibility for and perform all master and subordinate console operations:
  - A. Perform server administration functions
  - B. Issue operator commands
  - C. Perform periodic and emergency systems maintenance in accordance with procedures established to minimize the impact to DIR's and DCS Customers' businesses.
  - D. Perform system and service shutdowns and restarts, as required, and execute customary utility functions as per documented processes.
  - E. Maintain, administer, and provide necessary automated tools and processes for systems management.
  - F. Maintain tables, calendars, parameters, and definitions for tools used to automate manual procedures or to automate and improve the quality of the operations.

### 3.5. Production Control and Scheduling

The Successful Respondent must provide production control, scheduling and batch services for all in-scope environments leveraging tooling, services, API interfaces, and command line capabilities including, but not limited to:

- (i) Assume responsibility for production control and scheduling functions for both manual and automated production environments, including Batch accounts and Storage.
- (ii) Manage, maintain, monitor, schedule, complete, coordinate, communicate, and control online and batch process, both scheduled and unscheduled (including on-request processing in accordance with the established service level requirements and documented processes).

**State of Texas** Department of Information Resources, Data Center Services

- (iii) Schedule batch jobs within DIR and DCS Customer defined windows.
- (iv) Conduct annual review and continual improvement for non-automated batch work processes, including execution of automation functions wherever possible.
- (v) Investigate and report on all jobs, tasks and scripts that end abnormally if operations procedures require.
- (vi) Resolve interruptions caused by conditions external to production programs
- (vii) Execute re-runs to restart jobs, tasks, and scripts according to SMM.
- (viii) Identify job dependencies and create and maintain job dependencies.
- (ix) Develop, distribute, and obtain DCS Customers' approval of schedules prior to implementation.
- (x) Investigate and report on all jobs that end or perform abnormally.
- (xi) Create incident and/or problem records and or reports for job abnormalities.

### 3.6. Technical Services

#### 3.6.1. General Technical Support

Steady State Services include responsibilities and activities to support Public Cloud products and corresponding workloads including operating system instances, processes, systems management roles and services for IaaS, PaaS, SaaS, virtual networks (virtual private containers), microservices, container technologies, serverless architectures and other Public Cloud services. Responsibilities for the DCS environment including integration with other DCS providers to ensure availability of services. The Successful Respondent shall provide a Service that includes, but is not limited to:

- (i) Manage the implementation of Public Cloud products and services and related technologies to support required business applications.
- (ii) Support DIR and TSS SCP in Public and Hybrid Cloud framework and architecture design ensuring zones and regions are implemented in a manner to best meet DCS program needs and identifying potential issues in design or implementation that may adversely impact the DCS program.
- (iii) Provide technical support in accordance with SMM for operation including:
  - A. OS administration;
  - B. Virtualization of resources
  - C. Storage management;
  - D. Backup and recovery;
  - E. Disaster Recovery;
  - F. Physical and virtual server support;
  - G. Install/Move/Add/Change (IMAC);
  - H. Capacity planning and reporting;
  - I. Performance tuning;
  - J. Problem resolution and Root Cause Analysis; and
  - K. Configuration Management of products and services.
- (iv) Security compliance and integration into SIEM services.
- (v) Verify selected products and services are compliant with standards.
- (vi) Verify standardization and currency of software infrastructure and operating processes.
- (vii) Manage role-based access control following the principle of least privilege to ensure isolation of roles for business protection and audit purposes.

- (viii) Support the application lifecycle including performance optimization, capacity management and configuration management, including configuration and change management and auditing of configurations to ensure alignment with DIR defined standards. Where deviations exist, the Successful Respondent will notify DIR.
- (ix) Provide, test, and manage patches, fixes and version updates.
- (x) Provide and maintain service continuity planning and failover capabilities to ensure availability as defined DIR RPO/RTO requirements.
- (xi) Provide technical advice and support to Projects, applications, application development and database teams as required.
- (xii) Perform backups and restores of data and applications.
- (xiii) Enable and manage native Public Cloud services to allow for dynamic scaling to meet overall capacity needs.
- (xiv) Install, manage, and support Directory Services, including:
  - A. Manage authentication using Directory Services
  - B. Implement and manage trust relationships to new and existing domains
  - C. Add and remove objects from Directory Services as requested
  - D. Provide LDAP directory resources
- (xv) Design and implement user and system security measures in alignment with defined security policies.
- (xvi) Understanding and complying with the requirements of the DCS program and DCS Customers for configuration management items in the Service:
- (xvii) Design and implement AD and DNS configurations and settings that will allow for Public Cloud and Private Cloud hybrid integration.
- (xviii) Follow MSI-defined Incident Management processes leveraging the MSI-provided environment, currently ServiceNow;
- (xix) Track, monitor, and provide remediation for Service defects and incidents requiring system configuration or in-scope environment software or configuration changes;
- (xx) Implement and manage an automated software deployment and patching set of procedures and tooling leveraging Cloud best practices
- (xxi) Identify and implement required service or configuration changes to address solution defects;
- (xxii) Maintain service documentation (technical specifications and testing documentation) as well as common problems, root causes and remedy to aid in the identification and remediation of underlying system incidents;
- (xxiii) Participate in applicable acceptance testing or review of any changes arising as a result of break/fix or patch/release performed by Successful Respondent;
- (xxiv) Verify and ensure compliance with any DIR security mandated patches or configuration settings, or system levels to the extent and system enhancement turnaround time required given the nature of the security mandate and report to DIR, in writing, any risks or issues that the Successful Respondent becomes aware of in providing the Service to DIR.
- (xxv) Assist DIR and DCS Customers by referring incidents to the appropriate third-party entity for resolution and coordinating with the third-party service or service element provider as appropriate to help minimize the DCS Customer role in problem management.
- (xxvi) Implement measures to help avoid unnecessary recurrence of incidents impacting the Service, by performing root cause analysis and event correlation.
- (xxvii) Deliver support of environment for various Cloud Service Tiers as defined by Section 3.1.1 as agreed with DIR and authorized DCS provider users;

- (xxviii) Establishing, publishing, and maintaining a production calendar inclusive of daily and periodic maintenance activities;
- (xxix) Assess the utilization of all assets (Public Cloud products, platforms, storage, network interface points and the like) to:
  - A. Assist TSS and TPC SCP to utilize public cloud methods and expertise and apply public cloud techniques to the DCS private cloud environment including technology optimization, standardization and collaborative solutioning with DCS Customers to reduce complexity and drive higher levels of value and lower unit costs by service element; and
  - B. Utilize, within the defined lifecycle services within the DCS program, emerging products, and capabilities to more effectively deliver services;
- (xxx) Drive the overall consistency, repeatability and reliability of the Service through:
  - A. Simplification of service offerings and support tiers to move the Service to a support model that is highly repeatable and reliable;
  - B. Drive initial quality in service element implementations (e.g., “right first time”) and reduce I/P/C service requests wherever possible through implementation of repeatable templates, automation and utilization of programmatic orchestration;
  - C. Review of all DCS Customer-facing (and MSI-supporting) help channels and service reports to eliminate extraneous and conflicting elements including removing manual steps through the automation of I/P/C communications and processes;
  - D. Identify and eliminate recurring problems in the environment through automation of environment monitoring and alerts;
  - E. Automate data collection to drive better data and more timely data collection to facilitate Service decision making, cross functional coordination and long-term planning.
- (xxxi) Actively support the Demand Management process through development of technical solutions as initiated through Request for Solution procedures. This includes intra tower solution development as well as supporting TSS in development of intra-tower solutions.
- (xxxii) Perform analysis of and vetting of services and products across Public Cloud Providers and, in conjunction with TSS, develop service catalogs that are in line with DCS Program business assurance standards.
- (xxxiii) Develop and maintain support for cross platform cloud support solutions (e.g., Pivotal, OpenShift, etc.)
- (xxxiv) Provide enterprise file service support and management, including devices and appliances designed to provide remote file server functions.

### 3.6.2. Cloud Orchestration

The Successful Respondent will be required to deliver automated services from provisioning through retirement of services. These requests may be initiated from the MSI tooling and will be required to be executed following well-orchestrated procedures to provision, install, manage, secure in an automated manner. DIR currently owns licenses for ServiceNow Cloud Management Module and has implemented for Billing and CMDB updates, but have not yet completed Provisioning automation using this toolset. To ensure that services achieve the desired business and service-based outcomes, the Successful Respondent shall provide a Service that includes, but is not limited to:

- (i) Ability to integrate provisioning and management through automated orchestration and integration of Public Cloud Provider service catalogs (e.g. custom catalogs)

- (ii) Provisioning of infrastructure components, including compute, network, storage and security resources based on DIR defined Reference Architecture standards
- (iii) Extend IT ecosystem by integrating with Cloud native and third-party tools
- (iv) Integrate authentication and authorization for products and services
- (v) Ensure that security and certificates meet DIR program requirements
- (vi) Via tools and automation, create a single view of the enterprise to enhance customer experience, for operations and maintenance, and risk management/security capabilities
- (vii) Assist DIR and MSI in implementation of IT Financial Management (ITFM) billing and chargeback of services consumed within Public Cloud, including integrated tagging of services, products, and components for tracking chargeback.
- (viii) Perform necessary service integration within Successful Respondent Service Catalog to ensure necessary brokering, orchestration can occur in an automated fashion for successful provisioning of service requests.
- (ix) Support MSI in service integration in Service Catalog orchestration to ensure automated provisioning of requests
- (x) Enable a Shopping Cart experience to allow for seamless integration that can aggregate Public Cloud services consumption experience to see potential spend prior to procurement as well as track order fulfillment.

### 3.6.3. Cloud Mail and Office Productivity Application Services

To ensure that services achieve the desired business and service-based outcomes, the Successful Respondent shall provide a Service that includes, but not limited to:

- (i) Setup and Manage DCS Customer Cloud license/subscription request aggregating under the Public Cloud Provider Agreement.
- (ii) Monitor performance and conformance to SLAs under the Public Cloud Provider Service Levels.
- (iii) Conduct annual true-up and process monthly billing.
- (iv) As an optional service and upon request, provide technical support for customer initiatives such as migrations, interfaces, audits, DLP and other customer managed initiatives where SCP support, coordination or consulting may be required. These services would be provided through the Project Bench
- (v) As an optional service and upon request, evaluate and test compatibility and integration of new products/services or standards, architecture, and design with existing infrastructure and applications. These services would be provided through the Project Bench.

### 3.6.4. Performance and Capacity Management

To ensure that services achieve the desired business and service-based outcomes, the Successful Respondent shall provide a Service that includes, but is not limited to:

- (i) Actively participate in MSI work in developing performance and capacity management processes.
- (ii) Actively participate in exchange of data and information amongst MSI, other DCS Service Providers, DIR and Customers to ensure successful delivery of services, including ensuring the ability to validate capacity planning

- (iii) Integrate performance and capacity management tooling and process outputs with the MSI capacity management and other Service Management processes and systems
- (iv) Conduct performance and capacity planning and management activities for all supported products, platforms and applications.
- (v) Proactively monitor and manage performance and capacity of in scope systems, including identifying service issues that may impact the ability to delivery future services.
- (vi) Participate in scheduled capacity planning meetings.
- (vii) Creation, updating and reporting of a Capacity Plan which will include:
  - A. Developing an agreed upon formula for measuring capacity;
  - B. Services, components, and resources measured;
  - C. Current, trending and forecasted capacity based on technical currency planning, refresh activity as well as Demand Management;
  - D. Identify product or service (IaaS, SaaS, PaaS, etc.);
  - E. Detail performance and consumption characteristics;
  - F. Identify workload deployment type (Prod, Test, etc.);
  - G. Aggregate performance and consumption by product, cluster, pool, host, VM;
  - H. Identify trends and variances from previous reports;
  - I. Risk areas (including over and under capacity); and
  - J. Actual consumption compared to plan.
- (viii) Provide technical advice and support to Projects, applications, application development and database teams as required.

### 3.6.5. System Administration

The Successful Respondent must provide Systems Management and Administration Services for all in-scope service elements, including but not limited to:

- (i) Coordinating the installation, testing, operating, troubleshooting, and maintaining of the virtual networks (e.g. virtual private containers), compute resources, operating system(s), configuration items, software, appliances services, and other elements that comprise the Service;
- (ii) Actively support and assist the DCS Customer testing, review, and approval processes prior to the installation of these elements in a production environment; and
- (iii) Provision virtual servers as requested by DIR or DCS Customer.
- (iv) Execute the maintenance, Patching, and Support of the Operating System and hypervisors.
- (v) Assist in analyzing and correcting endpoint and/or network incidents and problems that may be associated with Server processing.
- (vi) Provide technical support for VM, storage and networking environments in the delivery of the service.
- (vii) Install productivity tools/utilities and perform all required operational modifications for the efficient and proper delivery of the Services.
- (viii) Identifying, testing, patch coordination and other updates associated with supported operating system(s), configuration items, hardware, software, appliances and other elements that comprise the Service.
- (ix) Implementing additional security-related fixes associated with the operating system(s), configuration items, software, appliances and other elements that comprise the Service;
- (x) Actively participate in the implementation of security and network protection solutions for the systems that are being managed by other DCS SCPs;

- (xi) Ensure that all solution delivery elements are maintained such that currency levels are maintained to be within vendor standard support levels;
- (xii) Ensure all Public Cloud hosted instances are tagged with necessary details to support billing, audit, reporting, security, and operations management to meet DIR and DCS Customer requirements
- (xiii) Ensure Secure Public Cloud hosted instances tagging cannot be altered by unauthorized users including customers.
- (xiv) Provide Public Cloud tagging enablement for provider managed tags based on predetermined rules and customer managed tags.
- (xv) Enable console access for DCS Customers to have visibility into services available as well as consumption for effective management resources. This includes API and CLI account access. These accounts should be governed by the principle of “least privilege” required to effectively support requirements to perform work responsibility.
- (xvi) Release upgrades for packaged infrastructure software are initiated through scheduled releases including, but not limited to: operating systems, patches, service packs, microcode, BIOS updates, virtualization software, virus scanners, etc.
- (xvii) Support Instance Schedulers to configure custom start and stop times within Public Cloud services to assist Customers to reduce operational costs.

### 3.7. Network Services

The Successful Respondent solution must provide networking services management for all in-scope service elements, including but not limited to:

- (i) Provide Enterprise Direct Connect solution to enable customers to securely connect to multiple Cloud Providers without having to establish direct connections between the individual DCS Customer and Cloud Provider.
- (ii) Provide Internet VPN connection option for use based on approved DIR use cases
- (iii) Provide Public Cloud Virtual Networking solutions supporting DIR and DCS Customer business, technical and security requirements.
- (iv) Architect VPC reference architecture standards which support customer segregation, billing, audit, reporting, security, and operations management.
- (v) Create and manage customer cloud environments using virtual networking reference architecture standards.
- (vi) Provide Public Cloud virtual network reporting (e.g., VPC/VNET, “Subnet In Use”, port mapping, Internet Usage).
- (vii) Provide a solution with the ability to control customer access to public cloud services and associated functions based on DIR approved policies and requirements. (i.e., ability to restrict/grant appropriate services access based on DIR approved services, support models and reference architectures). The solution shall be auditable and reportable enabling identification of levels of provider support services, console access granted with ability to correlate to Virtual Network (VPC/VNet) reference architecture standards and environment lifecycles.
- (viii) Provide and support VPC reference architecture standards as required by DIR which align with and support customer segregation, billing, audit, reporting, security, and operations management.
- (ix) Provide and support standardized VPC/VNet (or comparable) build automation and ability to support utilization of existing VPC's when required for new compute build request.
- (x) Provide and support ability to deploy custom VPC/VNet solutions.

**State of Texas** Department of Information Resources, Data Center Services

- (xi) Support and Assist Network SCP in design and management of direct Public Cloud network connections for delivery of services.
- (xii) Perform IP address allocation and management strategy in support of public cloud interoperability with private cloud.
  - A. Supports interoperability of multiple cloud provider and Private cloud environments
  - B. Support for IPv4 and IPv6

### 3.7.1. Web Application Firewall

The Successful Respondent solution must provide web application firewall management for all in-scope service elements, including but not limited to:

- (i) Solutioning and Provisioning WAF in support of customer requests including access management support
- (ii) Performing WAF configuration management support as required in coordination with customer application/business requirements in alignment with program security policies
- (iii) Performing operational and availability support of WAF services including log management and SIEM integration
- (iv) Performing WAF monitoring and alerting support including event response and integration with MSI and Security incident and event management systems and processes
- (v) Work with DCS Customer/SCP application teams to ensure alignment of security policies with business needs.
- (vi) Maintain awareness of Industry best practices and identified risks, including Open Web Application Security Project (OWASP) and incorporate into policy management lifecycle.
- (vii) Coordinate with other SCP's, DIR, and customers on development of Security Policy
- (viii) Enabling and performing integration with MSI systems and processes (i.e. Incident, change, CMDB) including management and use of WAF tagging

### 3.8. Storage Services

The Successful Respondent solution must provide Storage Management for all in-scope service elements, including but not limited to:

- (i) Architect, design, configure, monitor, and manage a robust and highly available storage solution to satisfy the overall needs of DIR and its Customers.
- (ii) Actively participate with MSI work in developing storage related management processes.
- (iii) Actively participate in exchange of data and information amongst MSI, other DCS Service Providers, DIR, and Customers to ensure successful delivery of services, including ensuring the ability to provide storage, backup, and recovery services.
- (iv) Develop and maintain strategies for the deployment and implementation across multiple service providers and platforms including integration with private and public cloud storage (i.e., archival), ensuring most cost-effective solutions and services are identified.
- (v) Design and manage Storage gateway solutions.

**State of Texas** Department of Information Resources, Data Center Services

- (vi) Identify opportunities for continual improvement, through knowledge management and skill review.
- (vii) Participate in and support scheduled disaster recovery tests.
- (viii) Assess and document DIR's current storage strategy and supporting environment across all Public Cloud providers to ensure that they collectively function as a cohesive group and perform as required and as to align with applicable SLAs and data protection standards.
- (ix) Perform environment/supported storage tuning, job and environment restructuring, and provide tools and other efforts to help improve the efficiency and reliability of storage and backup operations and to help reduce ongoing maintenance requirements.
- (x) Communicate appropriately with the DIR designees, DCS Customers, Authorized Users, DCS SCPs and third-party vendors as required to operate, maintain, and otherwise utilize the Service.
- (xi) Provide information and consulting support with respect to Service performance.
- (xii) Perform storage and backup Service testing, design appropriate test environments, and maintain backup system and Service documentation.
- (xiii) Provide management and monitoring of long-term archival solutions.
- (xiv) Implement encryption on all DCS storage in accordance with DIR requests.

### 3.8.1.Storage Operations

The Successful Respondent solution must provide Storage Operations for all in-scope service elements, including but not limited to:

- (i) Install tools and process to enable delivery of operations, monitoring, systems management, event response, and service restoration for the in-scope environment.
- (ii) Perform 7x24 monitoring, systems management, event response, and service restoration for the in-scope environment.
- (iii) Perform all event, warning, alert and alarm processing and management.
- (iv) Resolve all events, warnings, alarm messages and notify DCS Customers as appropriate.
- (v) Interface with Incident and Problem management processes and teams supporting resolution and service restoration.

### 3.9. Backup and Recovery Services

(a) Service element specific requirements that are pertinent to Backup/Restore and data loss prevention services as follows. In establishing, monitoring, and managing Backup/Restore Operations, the Successful Respondent will:

- (i) Architect, design, install, monitor and manage backup policies and services to satisfy the overall needs of DIR and its Customers within the Public Cloud and for support of hybrid solutions (i.e., Private cloud backup recovery to Public Cloud environment), including support for virtual machines, snapshots, virtual grids, virtual tape libraries (VTL), volumes, databases, tables, and filesystems.
- (ii) Identify areas in which Public and Private Cloud backup solutions can be leveraged to improve total cost of ownership and Disaster Recovery posture.
- (iii) Design and manage storage, file, tape and volume gateway solutions.
- (iv) Actively participate with MSI work in developing backup and recovery related management processes.

- (v) Coordinate all aspects of backup and recovery-based architecture, design, and planning throughout DIR.
  - (vi) Assess, develop, and formally recommend opportunities to reduce (or avoid) costs associated with backup environment.
  - (vii) Assess and document DIR's current backup strategy and supporting environment across all DCS Customers, inclusive of Public Cloud platforms used with devices, software, agents, job schedule, media, encryption and segmentation requirements, retention schedules and verification procedures to ensure that they collectively function as required and as to align with applicable SLAs and data protection standards.
  - (viii) Perform environment/supported backup tuning, job and environment restructuring, and provide tools and other efforts to help improve the efficiency and reliability of storage and backup operations and to help reduce ongoing maintenance requirements.
  - (ix) Maintain backup environments in accordance with DIR strategies, principles, and standards relating to technical, data and applications architectures as agreed-upon in this Exhibit, as required by DCS Customer projects or environments, or the run book or other supporting documents.
  - (x) Establish, publish and thereafter maintain a production backup calendar inclusive of daily and periodic backup and Service maintenance activities.
  - (xi) Generate and provide access to the MSI to daily production control and scheduling reports, including the production of monthly summary reports that track the progress of the Successful Respondent's performance of backup and Service maintenance work.
  - (xii) Implement encryption on all DCS Customer data maintained in any backup solutions in accordance with DIR standards.
  - (xiii) Perform ad hoc backup/restore operations reporting as agreed by the parties.
  - (xiv) Provide timely responses to DIR or MSI requests for information and reports necessary to provide updates to the DCS Customers and stakeholders. and
  - (xv) Meet with DIR Public Cloud backup Customers at least once annually to review existing backup schedules for suitability and to identify required updates to existing backup schedules and retention.
- (b) In addition to providing backups of in-scope services, provide for a Backup as a Service (BUaaS) solution for compute that is not in scope or managed by the Successful Respondent. This service is for current and discretionary DCS Customers that may or may not have servers in the consolidated data centers.

### 3.9.1.Backup Encryption and Key Management Requirements

As part of the Service, the Successful Respondent will, at all times:

- (i) Encrypt all backups, regardless of media and regardless of location (on/off DIR premise) ensure compliance per requirements of National Institute of Standards and Technology (NIST) Special Publication 800-53 (Rev. 4) SC-28 or successors. Details can be found at <https://nvd.nist.gov/800-53/Rev4/control/SC-28>; and
- (ii) Upon any return of Successful Respondent-created backup tapes or machine-readable media of DCS Customer data, the Successful Respondent will provide any encryption keys, passwords, hardware decryption keys (e.g., dongles) as necessary to decrypt the data and restore the data.

### 3.9.2.Backup Restoration Sampling and Testing Requirements

- (a) Monthly, the Successful Respondent will randomly select a sample from the DCS environment from each operating system group (e.g., Windows, Linux), each service element (e.g., database, OS) of backups maintained by the Successful Respondent to test the recoverability of the DCS assets that leverage the Backup/Restore Service. The following scenarios must be performed under this restoration test regimen:
  - (i) Simulating a failed virtual machine;
  - (ii) Simulating the loss of a home directory; and
  - (iii) Simulating the loss of a major file system.
- (b) The Successful Respondent will perform restoration services to demonstrate the efficacy of backup regimens in place. Should any restoration process fail or otherwise produce a defective result, the Successful Respondent will replicate the test on a second sample set.
- (c) Should the second sample set (or subsequent tests) fail, the Successful Respondent will:
  - (i) Immediately notify DIR that backup and/or restoration services are deemed unreliable;
  - (ii) Perform a detailed root cause and impact analysis as to include the scope, data sizes, timing, exposure, and duration that such conditions may have existed in the DCS environment;
  - (iii) Effect immediate repairs or replacement to the backup service elements that are the source(s) or potential source(s) of data backup or restoration issues that caused the unreliable condition;
  - (iv) Test and demonstrate to the DCS Customer that the Service has been restored in keeping with requirements; and
  - (v) Back-up the entirety of the Service elements (as a revised baseline) that failed or produced a defect with respect to restoration testing and perform a validation sampling test to demonstrate successful restoration services are performing to DIR standards.

### 3.9.3.Backup/Restore Operations

The Successful Respondent will:

- (i) Implement and monitor the backup/restore services operations for all regions and availability zones.
- (ii) Update the Backup platforms and services in use as new tools and technology are available that would improve DIR's or DCS Customers' business processes and performance
- (iii) Deliver operational support for the various service tiers (i.e., 24x7, compute processing (intermittent continuous operations on-demand)) production-availability schedule as agreed with DIR, the MSI, and DCS Customers or in accordance with the run book or other supporting documents;
- (iv) Verify backup outcomes correctly achieve provider service delivery requirements for provider responsible data (i.e., operating system recoverability);
- (v) Provide auditable solution for customer to view the schedule, retention, and target information as configured in the backup systems with ability for customer to correlate to customer's requested requirements;
- (vi) Provide reporting on backups and backup infrastructure (e.g., success/failure, schedules, retention, targets, archive, capacity, performance, storage media types and storage location);
- (vii) Perform backup administration and monitoring including:
  - A. Verify backup jobs start as scheduled;
  - B. Monitor scheduled production backup jobs;
  - C. Perform job restart, as necessary, in accordance with resolution and restart procedures;
  - D. Resolve backup scheduling conflicts; and

- E. Ensure that failed backup jobs are restarted once the condition of failure is identified and resolved.
- (viii) Monitor scheduler-related incidents and develop and recommend changes to the scheduler database;
- (ix) Schedule backup jobs, as requested by the DCS Customer, that require expedited or ad hoc execution;
- (x) Work with production staff (both the DCS Customers and SCPs) to create and adapt IT operational processes and procedures related to the backup of DCS environments;
- (xi) Perform successful backup processes in alignment to policies and procedures, customer requirements, service delivery availability and SLA requirements and provide notifications to DIR and DCS Customers as required;
- (xii) Support the ability of DIR and DCS Customers to sustain IT operations in the event of a disaster and loss of a facility by establishing and maintaining inter-data center data replication or off-site data replication; and
- (xiii) Perform DCS standard backup processes as follows, except where updated by DCS Customers as documented within their Schedules, Retention, and Targets document (SRT) (e.g. database log backup requirements).
- (xiv) The Successful Respondent will, for the backup/restore and data protection service elements of the overall Service:
  - A. Work with DCS Customers to transition to backup/recovery standards for all storage that includes on-premise (virtual tape), off-premise, and cloud-based backups as appropriate to the DCS Customer environment including database and file system snapshots, replication, and disaster recovery capabilities from public cloud providers;
  - B. Work with DIR in recommending backup/recovery services to non-customer entities and higher education as a risk mitigation service and an entry point into DCS; and
  - C. Sponsor and implement service evolution elements that include the use of containerization techniques to migrate DCS Customer workloads, configuration and data within the DCS Public cloud.
- (xv) Adhere to established procedures, timing, retention periods and frequency as documented in the SMM.

#### 3.9.4. Customer Specific Backup Scheduling and Retention Considerations

The Successful Respondent will review and continue to enable existing DCS Customer-specific backup schedules and backup retention periods as implemented for the Customer. As part of Ongoing Service Evolution and Optimization, the Successful Respondent will propose adjustments to DCS Customers for consideration that would result in both improvements to the customer's environment (e.g., backup coverage and retention) and better alignment to DCS standard backup strategies, processes, and services. The Successful respondent will not implement such improvements without the agreement of the DCS customer. Changes will be documented within the applicable SRT.

#### 3.10. Middleware Services

- (a) The Successful Respondent will be responsible for monitoring and management of defined resources for the Management and Operation of DIR's Middleware (e.g. MQSeries, WebSphere, etc.) environment. Middleware process monitoring is an optional service that customers may request. Support for standard

products are expected, and as technologies evolve, DCS governance may add new products to the standard products list.

- (b) The Respondent, as part of their proposal, and as the Successful Respondent providing the Middleware elements of the overall Service, shall:
- (i) Perform monitoring of defined Middleware environments.
  - (ii) Provide administrative support for Middleware (i.e. MQSeries) on all platforms used in DIR's and DCS Customers' environments.
  - (iii) Provide effective technical support (e.g. installation, patching, event resolution, advice, Third Party Vendor coordination) for middleware software required by the DCS Customers
  - (iv) Integration with DIR security monitoring and access control management standards (e.g., SIEM, Identity and Access Management (IAM)) as required by DIR via the DCS Security Service.
  - (v) Services to ensure that the billing and chargeback models applicable to the DCS Customer include all Service elements consumed and are presented to the DCS Customer with sufficient detail as to ensure completeness, accuracy and understanding of their consumption and charges for the Service.
  - (vi) Complete management of the lifecycle of provisioned middleware environments including specification, installation, implementation, monitoring and management, backup/restore and disaster recovery of DCS Customer middleware environments.

### 3.10.1. Middleware Process Operations

The scope and responsibilities of the Successful Respondent are as follows:

- (i) Provide system level performance statistics to the DCS Customer teams that are commonly available.
- (ii) Operational performance statistics summarized by DCS Customer and DCS Customer application(s)
- (iii) Monitoring and physical layer management of the Middleware systems components on 7x24 basis to ensure environments meet performance standards.
- (iv) Alerting of defined resources in the event of process, application, system events or thresholds have been exceeded. This notification will occur based on defined SMM procedures and agreed escalation matrix.
- (v) Monitor capacity and proactively provide performance and capacity planning.

### 3.11. Database Management Services

- (a) The Successful Respondent will be responsible for the management and operation of DIR's Public Cloud Database Management Services, inclusive of all database management systems across all Public Cloud providers available to DCS Customers. The Successful Respondent will provide these services over the duration of the agreement arising from this Exhibit based evolutions or alternates to the current database platforms as DIR determines. In addition to the requirements in this Section that are pertinent to all Public Cloud Services contained in this Exhibit, there are additional service element specific requirements. The Successful Respondent will be responsible for the Management and Operation of DIR's Texas Public Cloud Database Management Services (DBMS). As part of the next generation DCS, DIR seeks to utilize and

**State of Texas** Department of Information Resources, Data Center Services

integrate public cloud services (e.g. No-SQL, New-SQL, spatial, non-relational and streaming databases). These DCS services are collectively referred to DCS DBMS unless specific title-specific considerations are required. Database management is an optional service that customers may request. Support for standard product databases is expected, and as database technologies evolve, DCS governance may add new database products to the standard products list.

- (b) The Respondent, as part of their proposal, and as the Successful Respondent providing the DCS DBMS elements of the overall Service, will provide:
- (i) Perform physical database administration functions;
  - (ii) Deliver support of environment for various Service Tiers as defined by Section 3.1.1 Cloud Service Tiers for production availability schedule as agreed with DIR and authorized DCS provider users;
  - (iii) Complete management of the lifecycle of provisioned database environments including specification, implementation, monitoring and management, encryption, backup/restore, data protection restricted data identification, disaster recovery, data replication and decommissioning (e.g., archive, deletion, destruction) of DCS Customer databases;
  - (iv) An auditable security system that integrates database access control with the general security scheme for the enterprise, managed outside the project context and constantly kept up to date with respect to user status;
  - (v) Integration with DIR security monitoring and access control management standards (e.g., SIEM, Identity and Access Management (IAM)) as required by DIR via the DCS Security Service;
  - (vi) Services to ensure that the billing and chargeback models applicable to the DCS Customer include all Service elements consumed and are presented to the DCS Customer with sufficient detail as to ensure completeness, accuracy and understanding of their consumption and charges for the Service; and
  - (vii) Provide two levels of optional database management support services:
    - A. The Semi-Managed tier will include support for database availability, monitoring, maintenance, storage allocation, backup, patching, upgrades, and performance tuning support. The DCS Customer will retain responsibility for other logical database management functions such as DDL/DML, schema management, performance tuning, user management, and job scheduling functions.
    - B. The Fully-Managed tier will include the minimum levels offered in the Semi-Managed tier plus additional services in support of functions such as DDL, user management, and job scheduling functions. The DCS Customer would retain responsibility for logical DBA management such as DML and schema management functions.

### 3.11.1. DBMS Operations

The Successful Respondent will administer the following within the DCS DBMS platforms and in keeping with required SLAs per **Exhibit 1.2 Service Level Matrix**:

- (i) Provide system level performance statistics to the DCS Customer teams that are commonly available by Microsoft and Oracle-provided system consoles and functions inclusive of:
  - A. Operational performance statistics summarized by DCS Customer and DCS Customer application(s)
  - B. Root/DBA/Administrator (collectively Privileged Access) detailed reports including all:
    - 1. Privileged user accounts (listing) by DCS Customer;
    - 2. Bulk database operations including loading/unloading of data, database level changes to user/role profiles or access permissions; and
    - 3. Database and table creation(s) and deletion(s) activity.

- C. Monitor the DCS DBMS systems components on 7x24 basis to ensure databases meet performance standards including:
  - 1. Database and File system Servers/Services;
  - 2. Configure, schedule, and execute backups to storage in keeping with DCS Customer requirements, or in the absence of DCS Customer requirements as to align with DCS Environment Backup/Restore requirements as contained in Section 3.10
  - 3. Configure, schedule, and execute SQL Server Management Studio (SSMS) backups to storage within DCS Customer-provided storage and backup devices in keeping with DCS Customer requirements.
  - 4. Restore and recover data/files, in accordance with applicable services schedules upon receipt of an authorized DCS Customer service request.
- D. Monitor DCS DBMS capacity and proactively provide capacity planning
- E. Monitor all database objects (collectively static data, log and table spaces, indexes and the like) within the DCS DBMS and work with customers to identify all databases that may contain restricted data types within the CMDB. Restricted data types contain any data as restricted or controlled by Federal or State laws that contain any one of: HIPAA, FERPA, IRS-1075, PII, PHI, PCI, CJIS or any other restricted or sensitive data as identified by DIR. The MSI will produce a report, at the database level, by DCS Customer of all databases that contain such information on a monthly basis. For the avoidance of doubt, and as to ease the implementation of these requirements, if any database object contains any restricted data, the database (but not the underlying database objects) must be reported.

### 3.11.2. DBMS Administration

The Successful Respondent will administer the following within the DCS DBMS Service:

- (i) Manage the log files for the system processes for database programs; and
- (ii) Perform startup and shutdown of the system processes associated with system/platform software programs.
- (iii) Patch all components and system/platform software within the DCS DBMS System/Platform Monitoring
- (iv) Maintain and follow OEM developed software standards;
- (v) Manage OEM Application schemas;
- (vi) Perform OEM database space management;
- (vii) Perform database recovery, as directed by DIR;
- (viii) Provide performance tuning (Production environments) based on DCS Customer or DCS SCP direction, including tuning scripts or instructions;
- (ix) Perform database defragmentation upon request of the DCS Customer or DCS SCP or approval by the DCS Customer or DCS SCP should the Successful Respondent determine that proactive defragmentation is advisable;
- (x) Perform environment creation;
- (xi) Perform database refreshes;
- (xii) Perform database exports;
- (xiii) Provide OEM software server startup and shutdown functions using Microsoft, Oracle, IBM or OEM provided scripts;
- (xiv) Implement OEM technology stack updates (patches, updates, fixes, etc.) upon receipt of same from OEMs and the approval DIR.
- (xv) Perform database performance analysis

**State of Texas** Department of Information Resources, Data Center Services

- (xvi) Document files generated by the file management systems, including name, utilization statistics, and owning Applications.
- (xvii) Perform database stress testing, and operating system and database performance tuning.
- (xviii) Develop, document, and maintain physical database standards and procedures.
- (xix) Provide capability to achieve archiving and purging of historical or obsolete data from the production environments inclusive of databases, file, log, and swap space and other data stores prone to the accumulation of historical data.
- (xx) Actively participate in DIR's TSG governance committee to enable engagement towards setting of technology standards as to allow the Successful Respondent to adjust the skill composition of the team providing the DCS DBMS service in advance of the implementation and operation of such standards.

### 3.11.3. Texas DCS Database Standards and Evolution Requirements

The Successful Respondent is responsible for monitoring evolutions in database technologies (in general) and, as they relate to DCS, ensuring at all times that the appropriate staff maintains the knowledge, skills, certifications and experience as to design, implement, operate and maintain all DIR-identified DCS database standards over the duration of any agreement arising from this exhibit. These requirements may in the future, by way of examples and not as an exhaustive list or expression of DIR direction, include: NoSQL databases, NewSQL databases, Hadoop and evolutions; and graph databases; including commercial packages, distributions and open-source versions and variants. The Successful Respondent will participate in DIR's Technology Solution Group governance committee to enable engagement towards setting of technology standards as to allow the Successful Respondent to adjust the skill composition of the team providing the database service in advance of the implementation and operation of such standards.

## 3.12. Disaster Recovery Services

### 3.12.1. Disaster Recovery Overview and General Requirements

- (a) The MSI leads, manages, and oversees the Disaster Recovery Program (DR) within DCS, including Planning and Testing activities. Except as otherwise provided, DCS Customers will retain sole responsibility for overall business continuity plans. The Successful Respondent retains responsibility for business continuity plans for in-scope services and Public Cloud Platforms. The scope and responsibilities of the Successful Respondent are as follows:
  - (i) DR will apply to in-scope service elements located in the Public Cloud environment in consideration of existing capabilities and, following implementation, Successful Respondent Services to DIR;
  - (ii) Architect, design, install, monitor and manage DR services to satisfy the overall needs of DIR and its Customers within the Public Cloud and for support of hybrid solutions, including support for automated failover and testing.
  - (iii) Any Service elements that are under the scope and responsibility of the Successful Respondent in delivery of Services to Customers who elect to consume DR from the DCS program via the Successful Respondent;
  - (iv) All Successful Respondent services and Service support elements as required to operate and maintain the Services including all infrastructure and operational elements that the Successful Respondent provides or is dependent upon to deliver the Service to DCS Customers and, as applicable, other DCS SCPs;

- (v) Ensure that any existing implemented DR methods to enable specified DR/BC for DCS Customer applications and systems are not diminished as a result of Successful Respondent efforts;
- (vi) Designed and implemented to compliment DCS Customer activities in support of the DCS Customer’s overall DR and business continuity plan(s);
- (vii) Recovery of application environment and associated data. DR does not apply to middleware and application software configuration, application presentation, customizations, or extensions, and is limited to in-scope environment elements unless otherwise agreed to with DIR or DCS Customer;
- (viii) Enable DCS Customer and TSS SCP activities, processes and procedures for in-scope work and environments to deliver DCS Customer disaster recovery capabilities.
- (ix) Creation of a recovery service vault
- (x) Creation and management of VM backup policies and schedules to DIR and Customer standards
- (xi) Monitoring and remediation of backup failures on the Successful Respondent standard backup service
- (xii) Verification of validity of backup data and methodologies
- (xiii) Backup restoration testing
- (xiv) Installation, configuration, and management of file-level backup agents and service
- (xv) Provide input into DIR’s potential future specification, design and implementation of disaster recovery plans for in-scope environment elements, but exclusive of middleware, application or presentation software as agreed based upon the following principles:
  - (xvi) Leverage region failover and availability zones.
  - (xvii) Document procedures to restore primary operations for in-scope environment site operations (once available) within twenty-four (24) hours.
  - (xviii) Identification of redundant processing environment requirements to ensure 24x7 operations for DCS Customer-critical infrastructure components.
  - (xix) Specification of redundant power requirements to ensure 24x7 operations for DCS Customer-critical infrastructure components.
  - (xx) Specification of redundant networking requirements (network devices and telecommunications access) to ensure 24X7 operations for DCS Customer-critical infrastructure components.

(b) The following table is a summary of the scope and responsibilities of DR services:

**Table 4: Summary of Required Disaster Recovery Services**

DR Scope Area	Key Elements	Successful Respondent	DCS Customer	MSI
<b>Overall DR Planning and Testing (DCS Program)</b>	<ul style="list-style-type: none"> <li>■ DCS Program-level planning and coordination Services</li> <li>■ DCS Program Reporting</li> <li>■ DCS Program DR Enhancement / Optimization planning</li> </ul>	Participate	Participate	Lead
<b>DCS Customer Applications and Services</b>	<ul style="list-style-type: none"> <li>■ Customer Application (Executables, Binaries, Libraries and Services) unless otherwise requested</li> <li>■ Business Continuity Plans</li> </ul>	Responsible for Scripted or High Availability/Fault Tolerant (HA/FT) Services	Responsible	-
<b>DR Service Implementation</b>	<ul style="list-style-type: none"> <li>■ Design and Implementation of DR Services for DCS Customer Environments</li> <li>■ DR Implementation testing / validation</li> <li>■ Remediation of any detected DR defects or issues</li> <li>■ DR Operations</li> </ul>	Implement Operate Perform	Validate	Informed

DR Scope Area	Key Elements	Successful Respondent	DCS Customer	MSI
<b>Public Cloud Computing Elements</b>	<ul style="list-style-type: none"> <li>■ Computing Elements</li> <li>■ Servers/Appliances</li> <li>■ Storage</li> <li>■ Middleware Services</li> <li>■ Database Services</li> </ul> <p>As provided to: DCS Customers; any DCS SCP using Services contained in this Exhibit; and any DIR shared services customer or provider upon request. Scope includes both production and non-production (e.g., development, test) elements within the DCS program.</p>	Implement Operate Perform	Consulted  Validate	Validate
<b>Service Delivery Infrastructure</b>	All Successful Respondent provided Service Delivery elements including operational, security, network, monitoring and other elements as included in the Successful Respondent Service	Implement Operate Perform	-	Informed

### 3.12.2. Application Restoration/Resumption Services Requirements and Responsibilities

As part of the DR Service, the Successful Respondent will design and implement the following Application-level restoration/resumption options for DCS Customers and subscribing service providers:

#### 3.12.2.1. Automated/Scripted Application Restoration/Recovery

- (a) The DCS Customer (or subscribing service provider) in conjunction with the Successful Respondent will provide application(s) or service(s) restoration/recovery routines or scripts as to facilitate the restoration of application-level services in an automated or programmatic method as to restore operations following the declaration or determination of a disaster event. In such cases, the Successful Respondent will ensure the successful execution of such provided restoration/recovery methods and validate the application-level services have been restored to normal operations in consultation with the DCS Customer (or subscribing service provider).
- (b) **Highly Available/Fault Tolerant (“HA/FT”) Resumption.** The DCS Customer, in conjunction with the Successful Respondent will design, test and deploy a customized application/service level resumption or continuation of normal operations following the detection or declaration of a disaster event. DCS Customers HA/FT implementations must include the programmatic detection of outages or service disruptions that result in automated failover of application/services to an alternate region / availability zone.

#### 3.12.3. Other Disaster Recovery Requirements

- (a) The Successful Respondent’s responsibilities with respect to the DR/BC services include the following:
  - (i) Upon request, the Successful Respondent will participate in planning sessions, testing review sessions, and other meeting activities between DIR and a participating DCS Customer for in-scope Service elements.
  - (ii) Participation in DCS Customer activities, processes, and procedures for in-scope work and environments to enable DCS Customer disaster recovery capabilities to ensure that respective roles, responsibilities, processes and procedures of the parties are understood and documented to be contemporary with the then-current DR solution(s) in use by DCS Customers.

**State of Texas** Department of Information Resources, Data Center Services

(b) The Successful Respondent will enable DIR’s potential future specification, design, and implementation of infrastructure DR plans for in-scope environments and environment elements, but exclusive of application or presentation software as agreed based upon the following principles:

- (i) Identify redundant processing environment requirements to ensure 24x7 operations for DCS critical components;
- (ii) Specify redundant Service delivery requirements (Service devices and telecommunications access) to ensure operations for DCS critical infrastructure components.
- (iii) Texas Emergency Management Council
  - A. During major emergencies, the Council representatives convene at the State Operations Center to provide advice on and assistance with response operations and coordinate the activation and deployment of State resources to respond to the emergency. Generally, State resources are deployed to assist local governments that have requested assistance because their own resources are inadequate to deal with an emergency. The Council is organized by emergency support function, or groupings of agencies, that have legal responsibility, expertise, or resources needed for a specific emergency response function.

### 3.12.4. Disaster Recovery Classification

(a) The Successful Respondent’s responsibilities with respect to the DR Classification include the following:

- (i) Develop a methodology that DCS Customers may use at their discretion to assess the current state of an application, and identify specific steps required to elevate the application to a higher DR Class.
- (ii) Assist Customers in assignment of DR Classification.
- (iii) The Respondent, as part of their proposal to this RFO, will solution the DCS Disaster Recovery Service to offer the following options to DCS Customers or subscribing DCS SCPs. As the Successful Respondent to this RFO, the DR service elements will be designed, implemented, and tested to verify compliance with the following DR class requirements:

#### Disaster Recovery Class Requirements

DR Class	Recovery Time and Point Objectives	Use Cases	Solution Concepts	Cloud Diversity	Data Elements	Testing and Validation Scope
A	Near Real Time	Mission Critical	Application enabled	Multi-Region Active / Active	DB Services, Replication Services	MSI Scheduled, full testing annually, Component level quarterly
B	RPO: < 15m / RTO: <1h	Urgent Priority	Always live, typically agent or tooling based	Multi-Region	DB Services, Replication Services	MSI Scheduled, full testing annually
C	RPO: <4h / RTO: <8h	High Priority	Always live but with minimal effectiveness; scripted failover	Multi-Region	DB Services, Replication Services	MSI Scheduled, full testing annually
D	RPO: Backup or snapshot / RTO: <5d	Lower Priority	Backup and restore solutions of images, snapshots, file backups	Multi-Region	Cloud backup solutions	MSI Scheduled, Table-Top Test Annually
E	Best Efforts	Upon Request	Backup and restore solutions of images, snapshots, file backups	Multi-Region	Cloud backup solutions	MSI Scheduled, Table-Top Test Annually

(b) DCS Customers will only be able to sign up for DR Classifications that match their service capability.

### 3.12.5. Disaster Recovery Testing

- (a) The MSI will develop a DR test schedule annually that schedules DR tests periodically throughout the year. Customers are encouraged to test all applications with DR plans annually. The Successful Respondent will perform the following annually for each DCS Customer utilizing the 2 highest defined DR Classes as well as the elements utilized to deliver the Services in this to be defined Exhibit as a whole, biennially, and as a tabletop exercise annually for lowest priority workloads:
- (i) Establish, with the MSI, test objectives with each DCS Customer designed to verify that the in-scope Service elements will be available within the agreed upon timeframes contained in a business continuity plan as they pertain to in-scope Service elements;
  - (ii) Follow MSI established schedule for testing in-scope environment elements of the disaster recovery and business continuity plans relating to in-scope Service elements at least annually, or as requested by the DCS Customer, in support of DCS Customers, designees, any testing and recovery providers, and relevant DCS third-party service providers (including Cloud Service Providers) in accordance with the MSI;
  - (iii) Continue to operate and manage the in-scope Service elements during periodic disaster recovery tests; and
  - (iv) Execute an annual tabletop disaster recovery test on in-scope service elements located in the Public Cloud environment in consideration of existing capabilities and, following implementation, Successful Respondent Services to DIR.
- (b) The Successful Respondent shall not be responsible for, or quote or specify services associated with:
- (i) Providing alternate data processing facilities or capabilities to DIR or DCS Customer inclusive of data centers, networking, redundant or failover equipment and associated software; and
  - (ii) Development of detailed disaster recovery or business continuity plans for DIR or DCS Customer applications; these plans shall remain the sole responsibility of the DCS Customer that maintains the application.

### 3.13. Cloud Provider Sourcing Support Requirements

- (a) DIR has historically provided DCS Customers access to the following public cloud providers leveraging the contract vehicles noted below:
- (i) Amazon Web Services (AWS): Contracted through Atos IT Solutions and Service, Inc. under DIR contract DIR-DCS-SCP-MSA-002
  - (ii) Microsoft Azure: Contracted through DIR Cooperative Contract, managed by Atos IT Solutions and Service, Inc. under DIR contract DIR-DCS-SCP-MSA-002.
- (b) For all IaaS services, DIR may hold the agreement with the Public Cloud Provider. For all SaaS services hosted by a DIR approved Public Cloud Provider, the Successful Respondent will purchase the service on behalf of the Agency, who may hold the agreement with the Public Cloud Provider. For all SaaS purchases, the appropriate technical and security validations will need to be completed by the Successful Respondent and the SaaS product must be approved by DIR. For SaaS services not hosted in a DIR approved Public Cloud Provider, the Successful Respondent will not purchase the service, unless otherwise approved in writing by the DIR.

**State of Texas** Department of Information Resources, Data Center Services

- (c) For all PaaS services hosted by a DIR approved Public Cloud Provider, the Successful Respondent will purchase the service on behalf of the DIR. Currently, only PaaS services that are hosted by a DIR approved Public Cloud Provider are allowed. DIR reserves the right to change this restriction.
- (d) If DIR is the Agreement holder with the Public Cloud Provider, the Successful Respondent must demonstrate a detailed understanding of Public Sector procurement practices and standards, and must be independent from any supplier providing hardware, software, security, cloud or “as a Service” offerings to DIR either directly or via a reseller or agent. The Successful Respondent will work with DIR to add new public cloud providers (via general support, direct contract with Successful Respondent, DIR Cooperative Contract, or other contracting vehicle as directed by DIR) to the Service, distinguishing services offered in Commercial and Government clouds for all US regions, by providing the following:
  - (i) Procurement Services
    - A. Perform appropriate technical, administrative, and operational research to support proposal and contract development;
    - B. Conduct contract strategy meetings to identify issues and DIR or DCS Customer requirements, facilitate pricing discussions, and obtain senior leadership input on timelines and outcomes;
    - C. Draft contractual provisions based on strategy discussions, senior leadership input, and organizational needs and expectations;
    - D. Support and assist DIR in contract negotiations with public cloud providers ;
    - E. Support DIR in ensuring executed strategies minimize potential costs and risks and benefit DIR operational and service delivery performance;
    - F. Engage relevant stakeholders in negotiation decisions involving legal or regulatory requirements, contract standards and cost targets;
    - G. Manage and maintain Contract management details; and
    - H. Resolve supplier contracting issues that are not adequately aligned with DIR requirements;
  - (ii) Operational Services
    - A. Support DCS Customers in Request submission in Service Catalog;
    - B. Review Public Cloud Provider billing for DCS Customers;
    - C. Provide pricing transparency between charges incurred from Public Cloud Provider and those billed to DIR and DCS Customers;
    - D. Manage DIR and DCS Customer disputes with Public Cloud Provider;
    - E. Support incidents, outages and performance issues with Public Cloud Provider; and
    - F. Support DCS Customer, MSI and other SCP with events, issues and incidents related to Public Cloud Provider services.

- (e) If DIR has approved the Successful Respondent as the Agreement holder with the Public Cloud Provider, then such Public Cloud Provider Third Party Contracts shall be procured and maintained in accordance with the provisions specified in **MSA, Section 4.16 and [Article 3.3 Procurement Management](#)**.
- (f) Where the Successful Respondent is the direct contract holder, including any outsourcer arrangement with Public Cloud Provider, Successful Respondent will work with DIR to add public cloud providers to the Service where appropriate, distinguishing services offered in Commercial and Government clouds for all US regions, by providing the following:
  - (i) Procurement and Contract Services
    - A. Perform appropriate technical, administrative, and operational research for proposal and contract development;
    - B. Conduct contract strategy meetings to identify issues and DIR or DCS Customer requirements, facilitate pricing discussions, and obtain senior leadership input on timelines and outcomes;
    - C. Draft contractual provisions based on strategy discussions, senior leadership input, and organizational needs and expectations;
    - D. Perform and manage contract negotiations with public cloud providers;
    - E. Ensure that executed strategies minimize potential costs and risks and benefit DIR operational and service delivery performance;
    - F. Engage relevant stakeholders in negotiation decisions involving legal or regulatory requirements, contract standards and cost targets;
    - G. Manage and maintain contract management details, requirements and any needed contract changes;
    - H. Conduct cost efficiency reviews to identify Public Cloud Provider funding programs, discount programs, credits, and other marketplace levers to drive cost reductions and savings;
    - I. Upon DIR request, Successful Respondent will make best commercial efforts to Provide documentation regarding partner discounts and comparisons to Public Cloud Provider's price (e.g. MSRP and Enterprise Discount Plan);
    - J. Manage and monitor contracts with public cloud providers to ensure DIR is receiving services as required; and
    - K. Resolve supplier contracting issues that are not adequately aligned with DIR requirements;
  - (ii) Operational Services
    - A. Support DCS Customers in Request submission in Service Catalog;
    - B. Review Public Cloud Provider billing for DCS Customers;
    - C. Perform ongoing reviews and provide monthly reporting of in-depth analysis of cost, trends, and savings opportunities;

- D. Provide financial operations and management tasks to promote cost optimization for DIR and DCS Customers;
- E. Provide pricing transparency between charges incurred from Public Cloud Provider and those billed to DIR and DCS Customers;
- F. Reconcile Public Cloud Provider billing against Services provided within DCS program;
- G. Provide billing detail to MSI by Public Cloud provider and according to DCS customer invoice process;
- H. Issue Purchase Order and payments to Public Cloud Provider on behalf of DIR and DCS Customers;
- I. Manage DIR and DCS Customer disputes with Public Cloud Provider;
- J. Support incidents, outages and performance issues with Public Cloud Provider; and
- K. Support DCS Customer, MSI and other SCP with events, issues and incidents related to Public Cloud Provider services.

### 3.14. Critical Support Services

#### 3.14.1. Security Services

- (a) DCS Customers are responsible for application layer (and higher) system services and functions that build upon the infrastructure environment elements. The Successful Respondent shall not be responsible for the implementation of security services of these applications as these shall be retained by DIR via either the DCS Customer or other identified DCS Service Component provider.
- (b) The Successful Respondent must be responsible for maintaining the security of information in DCS public cloud environment elements under management and in accordance with the DIR security policy. The Successful Respondent will implement information security policies and capabilities as they satisfy DIR's requirements contained herein. The Successful Respondent's responsibilities with respect to security services must also include the following:
  - (i) Manage intrusion detection & prevention and Distributed Denial of Service (DDOS) including prompt DCS Customer notification of such events, reporting, monitoring and assessing security events;
  - (ii) Installation and integration of all Security tools and agents as to support reporting and alerting into the DCS SIEM;
  - (iii) Provide Zone Based Security with stateful filtering between isolated networks with stateful packet inspection to manage packet flows, ensuring only packets from known active connections are allowed to pass;
  - (iv) Provide vulnerability management services including supporting remediation for identified vulnerabilities for Service assets;
  - (v) Collaborate with the MSI, the Security SCP, and the Network SCP to create and maintain specific data feeds between the Successful Respondent monitoring tools, the SIEM, and ITSM tooling.

- (vi) Implement and manage information security policies, tools, and capabilities based on best practices and Security SCP guidance.
  - (vii) Provide security monitoring tools and log analysis solution for these tools in accordance with DIR and DCS Customers security requirements including integration capability with an Enterprise SIEM solution.
  - (viii) Ensure DIR IT Security Policy is followed which includes the development, maintenance, updates, and implementation of security procedures with the DCS Customer's review and approval, including physical access strategies and standards, ID approval procedures and a breach of security action plans.
  - (ix) Support DCS Governance and DIR Security Teams in the implementation, maintenance and updating of DCS data security policies, including DIR information risk policies, standards and procedures;
  - (x) Managing and administering access to the systems, networks, operating software, systems files and DIR and DCS Customer's data;
  - (xi) Supporting DCS Customers in implementation of programs to raise the awareness of DCS Customers and staff personnel as to the existence and importance of security policy compliance;
  - (xii) Installing and updating system security software;
  - (xiii) Maintain configuration management and log and document changes to network configurations.
  - (xiv) Enable role-based access to Public Cloud services and functions for customer and enterprise user roles.
  - (xv) Assigning and resetting privileged account passwords per established procedures;
  - (xvi) Providing DCS Customer access to create user IDs, suspend and delete inactive logon IDs, research system security problems and maintain network access authority;
  - (xvii) Assisting processing DCS Customer requested security requests;
  - (xviii) Performing security audits to confirm that adequate security procedures are in place on an ongoing basis, with the DCS Customer's assistance providing incident investigation support;
  - (xix) Providing environment and server security support and technical advice;
  - (xx) Developing, implementing, and maintaining a set of automated processes so that DIR and DCS Customer data access rules, as are not compromised; and where the Successful Respondent identifies a potential issue in maintaining an "as provided" DIR infrastructure element with the more stringent of a DCS Customer security policy (which may be Federally mandated or otherwise required by law), identifying to DCS Customers the nature of the issue, and if possible, potential remedies for consideration by the DCS Customer.
- (c) The Successful Respondent will support and comply with requests to conduct periodic security and privacy audits and generally utilizes members of the security team (both DIR and DCS Customers), Internal Audit, depending on the focus area of an audit. Should an audit issue be discovered the following resolution path shall apply:
- (i) If a security or privacy issue is determined to be pre-existing to this agreement, Successful Respondent will have responsibility to address or resolve the issue. Dependent on the nature of the issue, DIR may elect to contract with the Successful Respondent under mutually agreeable

terms for those specific resolution services at that time or elect to address the issue independent of the Successful Respondent;

- (ii) If over the course of delivering services to DIR under this Contract for environments the Successful Respondent becomes aware of an issue, or a potential issue that was not detected by security and privacy teams the Successful Respondent is to notify DIR as defined with the SMM.
- (iii) If over the course of the agreement a security or privacy issue arises, whether detected by DIR, a DIR auditor or the Successful Respondent, that was not existing within an environment or service prior to the commencement of ongoing run services associated with this agreement, the Successful Respondent shall:
  - A. notify DIR of the issue or acknowledge receipt of the issue within 24 hours;
  - B. within 48 hours from the initial detection or communication of the issue from DIR, present a potential exposure or issue assessment document to DIR Account Representative and the Security Team with a high-level assessment as to resolution actions and a plan;
  - C. within four (4) calendar days, and upon direction from DIR, implement to the extent commercially reasonable measures to minimize DIR's exposure to security or privacy until such time as the issue is resolved; and
  - D. upon approval from DIR implement a permanent repair to the identified issue at the Successful Respondent's cost; and
- (iv) For environments and services, all new systems implemented or deployed by the Successful Respondent shall comply with DIR security and privacy policies.

#### 3.14.2. Security Administration

The Successful Respondent must provide Security administration services for all in-scope service elements, including but not limited to:

- (i) Communicate the physical and logical Security management processes to SCP personnel.
- (ii) Implement the physical and logical Security functions in accordance with DIR Rules and the SMM.
- (iii) Identify and communicate any gaps between DCS and DIR security procedures and Public Cloud environments.
- (iv) Validate that proper segregation of duties exists in accordance with DIR Rules and the SMM.
- (v) During the implementation of changes or management of crises where it is not feasible to observe a proper segregation of duties, immediately inform DIR and the MSI of this fact and keep a record of all actions performed.
- (vi) Inform DIR and the MSI immediately if Supplier becomes aware of any vulnerability or weakness in the Services and recommend a solution or mitigation.
- (vii) Perform Privileged Account Management leveraging the tooling deployed and administered by Security SCP and ensuring the principle of "least privilege".
- (viii) Enable and manage single sign-on capabilities including integration across Public Cloud providers
- (ix) To enable DCS to drive higher levels of compliance and defense with respect to its security posture within the overall Service, the Successful Respondent will:
  - A. Evaluate program security and recommend improvements based on DIR policy, industry standards, and best practices. Evaluate tool and processes associated with server provisioning, Service integration and management, DIR inter-connection with public cloud elements and implementation of public cloud computing;

- B. Monitor all assets actively for security vulnerabilities, flaws, virus/malware and other elements that would undermine the security posture of DCS;
- C. Drive higher levels of data encryption across all elements of the service for data in flight and data at rest – particularly for those service elements that are prone to attack, those that include high numbers of records with sensitive data;
- D. Seek and work with MSI, DIR, and Security operations SCP to implement identity management, multi-factor authentication and leverage DCS programmatic fraud/intrusion detection for all trusted user ids (e.g., root, admin, dba) within the scope of Services;
- E. Actively participate in regular third-party penetration testing of all DCS assets regardless of where they are implemented on/off premise, remediate vulnerabilities for Successful Respondent Services and oblige the appropriate DCS service component provider to remediate issues within their scope of responsibility; and
- F. Actively participate in an annual security assessment which is managed by the MSI and remediate all vulnerabilities.

### 3.14.3. Protection of DIR Data

- (a) To protect DIR Data as described in this Agreement, in addition to its other duties regarding the handling of or interactions with DIR Data, the Successful Respondent will:
  - (i) Maintain in confidence any PII and SSI which it may obtain, maintain, process, or otherwise receive from or through DIR or DCS Customer in the course of the Agreement;
  - (ii) Use and permit its employees, officers, agents, and independent contractors to use any PII/SSI received from DIR or DCS Customer solely for those purposes expressly contemplated by the Agreement;
  - (iii) Not sell, rent, lease or disclose, or permit its employees, officers, agents, and independent contractors to sell, rent, lease, or disclose, any such PII/SSI to any third party, except as permitted under this Agreement or required by applicable law, regulation, or court order;
  - (iv) Take all commercially reasonable steps to (a) protect the confidentiality of PII/SSI received from DIR or DCS Customer and (b) establish and maintain physical, technical and administrative safeguards to prevent unauthorized access by third parties to PII/SSI received by the Successful Respondent from DIR or DCS Customer;
  - (v) Give access to PII/SSI of the State only to those individual employees, officers, agents, and independent contractors who reasonably require access to such information in connection with the performance of the Successful Respondent's obligations under this Agreement;
  - (vi) Upon request by DIR or DCS Customer, promptly destroy or return to DIR or DCS Customer in a format designated by DIR or DCS Customer all PII/SSI received from DIR or DCS Customer;
  - (vii) Cooperate with any attempt by DIR or DCS Customer to monitor the Successful Respondent's compliance with the foregoing obligations as reasonably requested by DIR or DCS Customer from time to time; and
  - (viii) Establish and maintain data security policies and procedures designed to ensure the following:
    - A. Security and confidentiality of PII/SSI;
    - B. Protection against anticipated threats or hazards to the security or integrity of PII/SSI; and

C. Protection against the unauthorized access to, disclosure of or use of PII/SSI.

3.14.4. Cloud Access Security Broker Implementation and Operations Requirements

- (a) The Successful respondent will assist DCS Security SCP and implement a DCS enterprise Cloud Access Security Broker (CASB) within the DCS for all State data and systems that are maintained in any public cloud infrastructure (IaaS), platform (PaaS) or software (SaaS) provider cloud. The DCS CASB will be implemented and thereafter operated and maintained to follow established DCS Security SCP standards and implemented to ensure that network traffic between DCS devices and any public cloud provider complies with the DCS and State of Texas (TAC 202) security policies and will provide real-time access via reports, dashboards and alerts. All alerts will be integrated with the DCS SIEM as operated by the DCS Security SCP and identify all uses, and alert on suspicious or inappropriate cloud application use across cloud platforms and identity unsanctioned use inclusive of restricted or protected data, network or application/service access of State data and systems maintained within public cloud providers.
- (b) The DCS CASB will include auto-discovery to identify cloud applications and data in use to identify high-risk applications, high-risk users and other key risk factors as determined by DIR or DCS customers who maintain or have access to restricted or protected data. Further the DCS CASB will be implemented to enforce the most stringent of applicable Texas Security, DCS Security Policy or DCS Customer specified security access controls, including: encryption; device and access profiling; and credential mapping when DCS Identity and Access Management (single sign-on) is not available or utilized on any public cloud provider platform within the scope of the Successful Respondent.
- (c) The DCS CASB will be implemented and thereafter operated and maintained by the Successful Respondent to:
  - (i) Identify what all cloud services are in use (approved, unapproved or “shadow”), by whom, and what risks they pose to the DCS program as well as DCS Customer data and systems maintained in public cloud providers;
  - (ii) Evaluate and validate the security controls and data protection standards implemented in public cloud services to ensure that they meet all required security and compliance requirements;
  - (iii) Include the use a database of cloud services and their security controls and an indication as to what controls are implemented or absent as to help DCS customers increase the security controls pertinent to their public cloud environment(s);
  - (iv) Protect DCS program and customer data in the cloud by preventing certain types of sensitive data from being uploaded, and encrypting and tokenizing data;
  - (v) Identify potential misuse of cloud services, including both activity from insiders as well as third parties that compromise or circumvent establish DCS standards pertinent to user accounts; and
  - (vi) Enforce differing levels of data access and cloud service functionality based on the user’s device, location, and operating system as well as “role” within the organization (e.g., privileged access, trusted access, operational access, end-user, or general public access).

(d) The specific responsibilities of the Successful Respondent will be to:

- (i) Design, implement, operate and maintain DIR CASB Standards pertaining to the scope, policies and standards associated with the DCS program (in general) and implementation requirement specifics for each public cloud provider used by a DCS customer within the DCS program;
- (ii) Seek and include DIR's input and collaboration in the implementation of established CASB requirements and standards for use by DCS customers via the MSI portal;
- (iii) Collaborate with the DCS Security SCP to ensure that all requirements and standards are implemented by the correctly and completely for program public cloud provider elements;
- (iv) Review the overall design and implementation specifics with DIR, impacted DCS customers and the DCS Security Provider for implemented system(s) to achieve CASB requirements;
- (v) Design and implement requirements for all necessary integrations for alerts, alarms, reports and dashboards as to ensure that DIR and DCS customers are provided the required information to ensure the correct configuration, implementation and operation of CASB elements for public cloud elements of the DCS program;
- (vi) Support DIR and the DCS Security SCP in acceptance testing and reviews of DCS CASB element(s) prior to DIR acceptance of same, and resolve any identified or documented deviations, defects or omissions from the scope of the DCS CASB as implemented; and
- (vii) Ensure that all required SIEM integrations are included and operating to specification on an initial (i.e., implementation) and ongoing (i.e., operations and maintenance in the steady-state run requirements) of the overall Security Service.
- (viii) The scope of the CASB will include, but not be limited to, for all public cloud infrastructure (IaaS), platform (PaaS) or software (SaaS) systems and applications:
  - A. Enforcement of data loss prevention policies and reporting of policy violations by DCS customers;
  - B. Detection of anomalous access attempts or successes that violate established CASB policies;
  - C. Identification of insider threats and compromised accounts;
  - D. Logging or capturing of detailed audit trails, by user or access, inclusive of privileged or administrative access accounts or processes; and
  - E. Enforcement of established DCS access control policies.

#### 3.14.5. IT Network Connectivity & Monitoring Requirements

The Successful Respondent must be responsible for ensuring the Service adheres to the network connectivity, security, and operations requirements of DCS. The Successful Respondent's responsibilities with respect to these requirements must include the following:

- (i) Adherence to DCS resource naming, numbering, and asset identification standards.
- (ii) Establishing secure channels between the Service elements and Network / Security functions of DCS, within Successful Respondent's environment elements only, to deliver managed

infrastructure services-- using managed, end-to-end IP Security (IPSec) encrypted VPNs or hardware-based stateful inspection firewalls as provided by the Managed DCS Network / DCS Security Operations Services SCPs;

- (iii) Event management and continuous monitoring of Service elements based on pre-defined parameters and thresholds and feeding of events into fault management, event correlation and SIEM tools within the DCS environment.
- (iv) Systems monitoring across system components including identifying unauthorized access to any Service element, and reporting outages via the DCS tool sets to the MSI;
- (v) Event correlation for fault managed devices and mapping of the relationship for multiple identified events;
- (vi) Providing engineering support for addressing, mediating and managing critical virtual hardware and software issues;
- (vii) Maintaining and providing documentation for the Successful Respondent's areas of responsibility as they relate to other DCS providers and the MSI and participating in maintaining overall documentation for those elements within the Successful Respondent's scope.
- (viii) Maintaining and supporting components within the Successful Respondent's areas of responsibility, including:
  - A. Supporting computing asset software required and provided protocols and security techniques as well as standard data access and transport techniques used within DCS;
  - B. Providing hardware and software maintenance for environment servers, operating system, database, middleware and DCS Service software products and ancillary components as required to operate the systems;
  - C. Tracking, managing, communicating, and supporting resolution of Service exceptions, and exceptions that may impact multiple DCS providers and/or DCS Customers; and
  - D. Evaluating and testing, in advance: Service and interface equipment including the configuration and installation of equipment that will be attached to, and will communicate over, DIR or DCS Customer network and security services.
- (ix) Supporting the provision of connectivity to the Successful Respondent Services and third-party/DCS Customer facilities and systems or other external networks; and
- (x) Supporting overall DCS acceptance procedures for installation and changes to the DCS environment, and for verifying restoration of availability following problems with DCS elements that impact the Services.

#### 3.14.6. Security Event Identification and Alerting Services

If the Successful Respondent determines that there is any actual, attempted or suspected theft of, accidental disclosure of, loss of, or inability to account for any regulated data including but not limited to, PII, SSI, FTI, etc. by the Successful Respondent or any of its subcontractors (collectively "Disclosure") and/or any unauthorized intrusions into the Successful Respondent or any of its subcontractors' facilities or secure systems (collectively "Intrusion"), the Successful Respondent must immediately:

**State of Texas** Department of Information Resources, Data Center Services

- (i) Investigate and determine if an Intrusion and/or Disclosure has occurred;
- (ii) Notify DIR or DCS Customer within two (2) hours of the Successful Respondent becoming aware of the unauthorized Disclosure or Intrusion;
- (iii) Fully cooperate with DIR or DCS Customer in estimating the effect of the Disclosure or Intrusion's effect on DIR or DCS Customer and fully cooperate to mitigate the consequences of the Disclosure or Intrusion;
- (iv) Specify corrective action to be taken; and
- (v) Take corrective action to prevent further Disclosure and/or Intrusion.

#### 3.14.7. Distributed Denial of Service Protection Services

The Successful Respondent will:

- (i) Work with DIR or DCS Customer to support the denial of communications to/from known malicious IP addresses;
- (ii) Ensure that the Public Cloud network architecture separates internal systems from DMZ and extranet systems;
- (iii) Require remote login access to use two-factor authentication;
- (iv) Support DIR or DCS Customer's monitoring and management of devices remotely logging into internal network; and
- (v) Support DIR or DCS Customer in the configuration of firewall session tracking mechanisms for addresses that access the Public Cloud.

#### 3.14.8. Information Security and Access Controls

(a) The Respondent shall provide its proposed approach for information security and access controls, specifically:

- (i) **Information Security**
  - A. Patching and vulnerability management of hardware, software, and other system components that comprise or are provided by the Respondent's proposed solution, and the ability to control enforcement of patching based on vulnerability criticality;
  - B. Auditability of both the physical location and logical isolation of any hosted service to ensure compliance with security policy;
  - C. Automated breach identification and any processes for breach mitigation, isolation, and reporting;
  - D. Self-service and automated tools for handling data spills of classified or other controlled information;
  - E. Ability to securely delete data in both unclassified and classified environments; and
  - F. Self-service tools to access data and analysis generated by threat detection systems. The ability to provide notifications and findings to system owners. The ability to provide raw logs to DCS Customers for analysis.

(ii) **Access Controls**

- A. Managing technical policies at all hierarchical identity levels from one account to all accounts globally, and the ability to control access to services and restrict configuration parameters;
- B. Highly granular attribute and role-based access control configuration, and the ability to assign permissions to roles in accordance with technical policies;
- C. Object and resource access control management, including data and resource tagging;
- D. Token-based and time-limited federated authentication allowing a user to assume a role within the cloud environment at all classification levels; and
- E. Indicate which access control capabilities are available via web interface, command line interface (CLI) application, and/or application programming interface (API).

(b) In addition, the Respondent shall describe its proposed physical architecture and implementation for classified/protected data, specifically:

- (i) Architecture for physically isolated infrastructure capable of providing classified IaaS and PaaS services with functional parity to unclassified offerings; and
- (ii) Classified services are globally accessible, highly available, and can handle DCS Customer traffic, storage, and computing in accordance with the SLAs in Section 6.

### 3.14.9. Real Time Forensics Acquisition

- (a) Real time forensics acquisition is a service in which DIR would request that Successful Respondent implement a capability to accelerate the overall process of securing, acquiring and preserving evidence data within the Public Cloud and allows 3rd party forensic teams to perform analysis without potentially losing critical data.
- (b) The Successful Respondent shall:
  - (i) Implement and manage a forensics capability within any defined Public Cloud hosting environment.
  - (ii) Support DIR or SCP in securing, acquiring and preserving evidence data within the Public Cloud hosting environment.
  - (iii) Provide a mechanism to allow 3<sup>rd</sup> party forensics team access to collected data to perform analysis.

## 3.15. DIR Requested Projects

### 3.15.1. Procedures and Performance

Successful Respondent will perform Projects as directed by DIR, in accordance with the terms of this Agreement and the process described in this Section. From time to time and at DIR's sole discretion, DIR may request Successful Respondent to perform Projects. DIR may initiate a request for a new Project by providing such request in writing (each such request, a "Project Request") to Successful Respondent. Successful Respondent shall justify to DIR when it has insufficient resources to perform such work, including through reprioritization or **State of Texas** Department of Information Resources, Data Center Services

rescheduling of Project activities of Successful Respondent Personnel. The Designated DIR Representative will request, define and set the priority for Projects. Successful Respondent shall maintain appropriate continuity of personnel assigned to perform Projects.

### 3.15.2. Project Work Order

- (a) Successful Respondent shall, within the time frame specified in such Project Request (and in no event more than five (5) DIR Business Days from receipt of such request unless another time frame is approved by DIR), at no charge to DIR, prepare and deliver to DIR a proposed Project Work Order (each, a "Project Work Order"), as described below. Each proposed Project Work Order prepared by Successful Respondent will contain the following information:
- (i) a detailed description of the scope of work to be performed by Successful Respondent to complete and implement the Project, including any required Deliverables;
  - (ii) any specific performance standards that will apply to the completion and implementation of such Project, including Successful Respondent's agreement to meet applicable Service Levels;
  - (iii) an anticipated schedule for completing and implementing the Project and any related Deliverables, including Milestones and credits for failing to achieve Acceptance of Milestones and Deliverables;
  - (iv) a description of the Successful Respondent positions that will be assigned to each activity specified in the Project Work Order, including the location of Successful Respondent Personnel assigned to such positions (i.e., onsite, offsite, onshore and sufficient detail to allow DIR to audit the assignment and billings related to such Successful Respondent Personnel;
  - (v) a description of the Acceptance Criteria and Acceptance Testing procedures to be used by DIR in connection with any Acceptance Testing of such Project and any related Deliverables and Milestones;
  - (vi) the estimated number of personnel hours needed to complete the Project;
  - (vii) one (1) or more fee quotes, based on the following pricing mechanisms:
    - A. the applicable hourly rate, in accordance with the Rate Card,
    - B. if the Project consists of multiple units of work for which there are pre-defined one-time Charges, the number of pre-defined work units multiplied by the applicable pre-defined one-time Charge, or
    - C. if requested by DIR, a fixed fee or other pricing mechanism.
  - (viii) DIR may, at its option, choose which pricing mechanism will apply to the Project.
- (b) Successful Respondent will not commence performing any services in connection with a Project, and DIR will not be responsible for any Charges applicable to such Project, until the Parties have executed the applicable Project Work Order. Any change to a Project Work Order will be made pursuant to the Change Control Procedure.

### 3.15.3. Approval of Projects; DIR and DCS Customer Requests

The Designated DIR Representative may accept or reject Project proposals in his or her sole discretion. Successful Respondent shall not agree to provide Projects to DIR or any DCS Customers without the prior approval of Designated DIR Representative. DIR shall not be obligated to pay for any Projects not properly authorized by the Designated DIR Representative. Without limiting DIR's other rights under this Agreement or applicable Law, if Successful Respondent fails to comply strictly with this Section, it shall receive no compensation for any services rendered to DIR or any DCS Customer in violation of this Section.

#### 3.15.4. Reprioritization, Termination, and Suspension

Successful Respondent acknowledges and agrees that DIR will have the right based on valid business reasons to reprioritize, terminate, or suspend any Project at any time upon informing the Successful Respondent Contract Manager. DIR will not be obligated to pay Successful Respondent any additional compensation associated with such action unless the corresponding Project Work Order expressly provides otherwise. If DIR decides to terminate a Project Work Order, Successful Respondent will stop performing the Project work in an orderly manner as of the date specified by DIR, and Successful Respondent will only be entitled to charge DIR for actual performance provided by Successful Respondent for chargeable Project work up to the date specified in DIR's notice.

#### 3.15.5. Demand Management

The Successful Respondent will identify project resources by skill type and will enter staff availability into the MSI's demand management system. The Successful Respondent will assign those resources to the solution requests and project implementations. The staff will estimate work effort in hours to both solution and implement requests and will track these estimates in the MSI's demand management system. The staff will then track actual hours spent by project in the MSI's demand management system.

#### 3.15.6. Demand Management Forecasting and Reporting

- (a) The Successful Respondent will use the MSI demand management resource planning tool to provide a schedule of project hours consumed (by DCS Customer activity, resource type, and Project) to forecast requested projects. The Successful Respondent will use the MSI tool to demonstrate accurate estimating and staff allocation to projects such that deadlines are met. Successful Respondent will also participate in project staffing and resource assignment meetings as requested.
- (b) Two (2) SLAs will report Successful Respondent timeliness and quality of project delivery:

##### 3.15.6.1. Solution Proposal Delivery

The Successful Respondent will assess the complexity of DIR's solution request as defined by the SMM. The complexity will determine the Solution Proposal SLA due date, which may be adjusted with sufficient justification by mutual agreement of the Successful Respondent and DIR.

##### 3.15.6.2. Solution Implementation

The Successful Respondent and DIR will mutually agree on the solution implementation date based on the Successful Respondent's estimated scope and proposed implementation date. This solution implementation date may be adjusted with sufficient justification by mutual agreement of the Successful Respondent and the customer.

### 3.16. Reporting

As part of the Service, the Successful Respondent shall:

- (i) Generate and provide access to DIR and MSI to daily production control and scheduling reports, including the production of monthly summary reports that track the progress of the Successful Respondent's performance of maintenance work (details are contained in **Appendix A Reports**).

**State of Texas** Department of Information Resources, Data Center Services

- (ii) Provide all current state reports as described in **Appendix A Reports** and required in sections **6. Performance Model – Service Level Agreements**, and **9. Cross-Functional Services**.
- (iii) Perform in-scope ad hoc operations reporting as directed by DIR.

### 3.17. Quality Assurance

- (a) The Successful Respondent will be responsible for adhering to quality assurance processes and procedures developed by the MSI. Successful Respondent should provide documentation related to its approach for ensuring continuous quality assurance processes and procedures for the delivery of Services including:
  - (i) Confirming compliance with agreed upon quality assurance procedures;
  - (ii) Conducting quality and progress reviews with appropriate DCS Customer personnel;
  - (iii) Supporting MSI with developing and publishing a quality assurance/quality control (QA/QC) manual;
  - (iv) Verifying compliance with the published QA/QC manual;
  - (v) Maintaining Service equipment and software quality consistent with its obligations; and
  - (vi) Documenting and implement process improvement including identifying industry leading practices.
- (b) Successful Respondent shall develop and implement Quality Assurance and internal control (e.g., financial and accounting controls, organizational controls, input/output controls, system modification controls, processing controls, system design controls and access controls) processes and procedures, including implementing tools and methodologies, to perform the Services in an accurate and timely manner (and confirm that they are so performed and accounted for) in accordance with (1) the Service Levels and other requirements of this Agreement, (2) Generally Accepted Accounting Principles (US GAAP) to the extent necessary for Successful Respondent to make its public filings with the Securities and Exchange Commission, (3) accepted industry standards of first tier providers of services that are the same as or similar to the Services, (4) the Laws applicable to DIR and the DCS Customers (without limiting the obligations of the Parties under MSA Section 8.11 Compliance with Laws, and (5) industry standards (e.g., QS 9000, ISO 9001/2000, ISO 14000, ISO 17799/2005, ISO 27001/2005, ISO 27002/2005) applicable to DIR and the performance of the Services to the extent described in Section [3.18 Industry Standards, Certifications and Compliance](#). Such processes, procedures and controls shall include verification, checkpoint reviews, testing, acceptance and other procedures for DIR and the DCS Customers to assure the quality and timeliness of Successful Respondent’s performance. Without limiting the generality of the foregoing, Successful Respondent shall:
  - (i) Maintain a strong control environment in day-to-day operations to assure that the following fundamental control objectives are met:
    - A. financial, billing and operational information is valid, timely, complete and accurate;
    - B. operations are performed efficiently and achieve effective results, consistent with the requirements of this Agreement;
    - C. assets and data are safeguarded in accordance with Successful Respondent’s own internal (and in all events reasonable) practices (but without expanding Successful Respondent’s obligations under **MSA Section 6.2.2 Safeguarding of DIR Data**); and
    - D. actions and decisions of the organization are in compliance with Laws (without limiting the obligation of the Parties under Section [3.18 Industry Standards, Certifications and Compliance](#)) and the terms of this Agreement;

- (ii) Build the following basic control activities into work processes:
    - A. accountability clearly defined and understood;
    - B. access properly controlled;
    - C. adequate supervision;
    - D. transactions properly authorized;
    - E. transactions properly recorded;
    - F. transactions recorded in proper accounting period;
    - G. policies, procedures, and responsibilities documented;
    - H. adequate training and education; and
    - I. adequate separation of duties;
  - (iii) Perform periodic control self-assessments with respect to all Services as necessary to ensure compliance;
  - (iv) Maintain an internal audit function to sufficiently monitor the processes, internal controls and Systems used to provide the Services (i.e., perform audits, track control measures, communicate status to management, drive corrective action, etc.) and provide copies of any such internal audit reports to DIR upon request; and
  - (v) Conduct investigations of suspected fraudulent activities within Successful Respondent's organization that impact or reasonably could be expected to impact DIR or the DCS Customers. Successful Respondent shall promptly notify DIR of any such suspected fraudulent activity and a reasonable summary of the results of any such investigation as they relate to DIR or the DCS Customers and such supplemental materials as DIR may reasonably request. At Successful Respondent's request, DIR shall provide reasonable assistance to Successful Respondent in connection with any such investigation.
- (c) Successful Respondent shall submit such processes, procedures and controls to DIR for its review, comment and approval as part of the SMM process and shall use commercially reasonable efforts to finalize such processes, procedures and controls and obtain DIR's final approval on or before the established due date. Upon DIR's approval, such processes and procedures shall be included in the Service Management Manual. Prior to the approval of such processes and procedures by DIR, Successful Respondent shall adhere strictly to DIR's and the DCS Customers' then-current policies, procedures and controls. No failure or inability of the quality assurance procedures to disclose any errors or problems with the Services shall excuse Successful Respondent's failure to comply with the Service Levels and other terms of this Agreement.

### **3.18. Industry Standards, Certifications and Compliance**

Successful Respondent shall comply with TAC 202, PCI, HIPAA, MARS-E, IRS 1075, CJIS, SSA, ISO 9000, ISO 9001:2000, ISO 14001, ISO 27001/2005, and ISO 27002/2005 and shall apply ITIL standards and Six Sigma processes.

#### **3.18.1. SOC 2 Reports**

- (a) In addition to its other obligations under this Section, Successful Respondent shall cause a Service Organization Controls 2 Report, type II, [{"SOC 2 Report"}] (SOC 2: Attestation Standards, Section 101 of the AICPA Codification Standards (AT Section 101), "Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2)", as published by the AICPA in 2011] to be conducted by an independent, nationally recognized public accounting firm qualified to perform such audits at least annually, prepared in accordance with the relevant and current standards. The

Successful Respondent acknowledges that each such SOC 2 Report shall cover Successful Respondent's policies, procedures, controls and systems for twelve (12) months of Successful Respondent's performance of the Services, in accordance with the State fiscal year (and each successive twelve (12) month period thereafter unless otherwise agreed to), and in particular those policies, procedures, controls and systems applicable to an audit of Successful Respondent's customers. Prior to initiating any such SOC 2 Report, Successful Respondent shall confer with DIR as to the scope and timing of each SOC 2 Report and shall accommodate DIR's requested modifications (if any) for each such SOC 2 Report to the extent reasonably practicable.

- (b) Successful Respondent shall cause its Subcontractors performing the Services to allow SOC 2 Reports on their policies, procedures, controls and systems that complement the SOC 2 Report performed pursuant to clause (1) above, when requested by Successful Respondent, DIR, Customers, Texas State Auditor's Office, and other entities authorized by DIR. If Successful Respondent is unable to cause its Subcontractors to conduct such SOC 2 Reports or chooses to conduct the SOC 2 Reports of such complementary policies, procedures, contracts and systems itself, then Successful Respondent shall engage an independent, nationally recognized public accounting firm to perform such audits of its Subcontractors to ensure that the policies, procedures, controls and systems of the Subcontractor complement those of Successful Respondent. For purposes of this clause (2), the term "complement" shall mean that the policies, procedures, controls and systems of the Subcontractors, when taken as a whole in combination with the policies, procedures, controls and systems of Successful Respondent, represent the entire control environment under this Agreement.
- (c) Unless otherwise agreed by the Parties, a copy of the final annual report dated December 31st will be provided by Successful Respondent to DIR and DIR Auditors ten (10) Business Days from the date Successful Respondent receives the final report from the external firm. In all events, each report delivered by such date shall be unqualified and Successful Respondent shall respond to such report in accordance with **MSA Section 4.12 Audit Rights**. In addition, within ten (10) Business Days of DIR's written request to Successful Respondent, Successful Respondent shall provide a letter to DIR signed by an officer of Successful Respondent certifying that there has been no change in the policies, procedures, controls and systems of Successful Respondent since the date of the most recent SOC 2 Report.
- (d) To the extent DIR provides notice and requests that, in addition to the SOC 2 Reports described in clauses (1) and (2) above, Successful Respondent conduct DIR-specific SOC 2 Report, Successful Respondent shall, at DIR's expense, cause such DIR-specific SOC 2 Report to be performed by a nationally recognized public accounting firm qualified to perform such Report; provided, however, that Successful Respondent timely notifies DIR of such expense, obtains DIR's prior written approval and uses commercially reasonable efforts to minimize such expense. A copy of the final report of each such DIR-specific SOC 2 Report shall be delivered to DIR by Successful Respondent ten (10) Business Days from the date Successful Respondent receives the final audit report from the external firm. If Successful Respondent undertakes additional or different SOC 2 Reports (other than customer-specific audits requested and paid for by other Successful Respondent customers), Successful Respondent shall accord DIR the rights described in clause (1) above with respect to such reports. To the extent DIR provides notice and requests that, in addition to the SOC 2 Reports described in clauses (1) and (2) above, DIR may, in coordination with the DIR Auditors, conduct DIR-specific SOC 2 Report on the services facility at or from which the Services are provided.
- (e) During the period when SOC 2 Reports are performed under this Section, Successful Respondent shall provide DIR with periodic updates on the status of such reports and any issues that are specific to DIR or that are reasonably anticipated to impact in any material respect the control environment under this Agreement. Upon completion of any such SOC 2 Report that identifies any significant deficiency or material weakness, Successful Respondent shall prepare and implement a corrective action plan to correct any such deficiency or

resolve any problem identified from such SOC 2 Report specific to DIR or that impact in any material respect the control environment under this Agreement. A copy of the corrective action plan shall be provided to DIR within thirty (30) days following the discovery of such deficiency or problem. If the SOC 2 Report shows a control issue that is specific to DIR or that impacts in any material respect the control environment under this Agreement (a "Control Deficiency") that has not theretofore been corrected or properly mitigated and such failure to mitigate the Control Deficiency leads to a qualified opinion being issued by Successful Respondent's auditor, then Successful Respondent's failure to promptly remedy the Control Deficiency will be deemed a material breach of this Agreement triggering a termination rights for DIR under **MSA Section 13.1 Termination for Cause**.

- (f) If Successful Respondent is unable to timely deliver to DIR any report described in this Section that does not identify any significant deficiency or material weakness, Successful Respondent shall:
- (i) provide a certificate from an officer of Successful Respondent to DIR certifying, on the date such report is delivered, or is otherwise due to be delivered, the circumstances giving rise to any delay in delivering such report,
  - (ii) promptly take such actions as deemed necessary by DIR to resolve such circumstances and deliver such report as promptly as practicable thereafter, and
  - (iii) permit DIR and the DIR Auditors (or their agents), at Successful Respondents' expense, to perform such procedures and testing of the operating effectiveness of Successful Respondent's policies, procedures, controls, and systems for the period otherwise covered by such report.

### 3.18.2. Audit Requirements

- (a) DIR, DCS 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. The Successful Respondent shall cooperate with audits DIR requires.
- (b) Successful Respondent shall provide corporate security policies in addition to DCS security policies if required for an audit.

### 3.19. Obligation to Evolve

- (a) Successful Respondent shall identify and propose the implementation of services, products and offerings that are likely to: (i) improve the efficiency and effectiveness of the Services (including cost savings); (ii) improve the efficiency and effectiveness of the processes, services and related functions performed by or for DIR and the DCS Customers; (iii) result in cost savings or revenue increases to DIR and the DCS Customers in areas of their operations outside the Services; and (iv) enhance the ability of DIR and the DCS Customers to conduct their operations and serve their constituencies and customers faster and/or more efficiently than the then-current strategies. Successful Respondent will cause the Services, Software and other assets used to deliver the Services, as approved by DIR, to evolve and to be modified, enhanced, supplemented and replaced as necessary for the Services, Software, and other assets used to deliver the Services to keep current with industry best practices and a level of technology that is:
- (i) compliant with all Laws applicable to the provision and receipt of the Services;

- (ii) used by Successful Respondent and other top-tier IT providers in providing services similar to the Services to other customers; and
  - (iii) in general use within the IT industry.
- (b) Any changes to the Services, Software, and other assets used to deliver the Services implemented in accordance with this Section will be deemed to be included within the scope of the Services to the same extent and in the same manner as if expressly described in this Agreement, at no additional charge to DIR.

#### 3.19.1. Flexibility

The technologies and process strategies Successful Respondent employs to provide the Services shall meet industry standards and shall be flexible enough to allow integration with new technologies or processes, or significant changes in DIR's or a DCS Customer's objectives and strategies. For example, Equipment must have sufficient scalability and be sufficiently modular to allow integration of new technologies without the need to replace whole, or significant parts of, systems or processes (e.g., made to be a one-to-many model) to enable DIR's and/or the DCS Customers' operations to become more scalable and flexible.

#### 3.19.2. Obligation to Identify Best Practices

Throughout the Term, Successful Respondent shall (1) identify and apply best practice techniques, methods and technologies in the performance of the Services; (2) train Successful Respondent Personnel in the use of new techniques, methods, and technologies that are in general use within Successful Respondent's organization and the IT and business consulting industries; and (3) make necessary investments to keep and maintain the Software and other assets used to deliver the Services at the level of currency defined in this Section.

#### 3.19.3. Successful Respondent Briefings

Successful Respondent will meet with DIR at least once during every 180-day period throughout the Term to inform DIR of: (1) any investments, modifications, enhancements, and improvements that Successful Respondent is required or proposes to make to the Services, Software, and other assets used to deliver the Services pursuant to this Section; (2) new information processing technology or business processes Successful Respondent is developing; (3) any pending or actual changes in Law that could reasonably be expected to affect the provision or receipt of the Services; and (4) technology or process trends and directions of which Successful Respondent is otherwise aware that could reasonably be expected to have an impact on DIR's IT operations or business.

### 3.20. Operating Agreements with Other SCPs and MSI

- (a) DIR holds other contracts for additional or related work for the DCS SCPs, platforms and customer specific projects and services. The Successful Respondent must fully cooperate with the MSI and all other DCS SCPs as may be required for the smooth and efficient operation of all related or additional work arising from this Exhibit. The Successful Respondent may not act in any way that may unreasonably interfere with the work of any other DCS participant or DIR or DCS Customers' employees. Additionally, the Successful Respondent must include the obligations of this provision in all its contracts with its subcontractors that work on any Project or Service arising from this Exhibit.
- (b) Mutually supportive relationships among DCS SCP, in addition to relationships with DIR and the MSI, are required to deliver a seamless and well managed service to DCS Customers.

(c) The Successful Respondent is required to enter into Operating Agreements (OAs) with the MSI and SCP including but not limited to mainframe, print/mail, public cloud, network, and security, and future SCPs should DIR identify them to the Successful Respondent. The Successful Respondent will contribute to the design of these OAs, and will be responsible for implementing, following and responding to these agreements once developed. At a minimum, these OAs will include SCP to SCP agreements that address processes, protocols, and communications for:

- (i) Joint operation, issue resolution, and governance of the delivery of Services;
- (ii) Customer support functions for multi-service provider solution requests;
- (iii) Incidents resolution and project management for multi-service provider escalations;
- (iv) Operations management;
- (v) Security matters including active or persistent threats and multi-party response/remediation functions;
- (vi) The Successful Respondent and the MSI and SCPs will acknowledge and agree in the OA that the Successful Respondent will assist and coordinate the delivery of Services to DIR and DCS Customers. In addition, the Successful Respondent, MSI and SCPs shall each promptly disclose to the other any material difficulties or delays that either experiences in connection with the delivery or operation of the Services;
- (vii) Ensuring consistent levels of quality in the DCS environment while providing transparency across all levels of the DCS service component provider organization, to DCS Customers, the MSI and DIR;
- (viii) Defined and agreed standards of accountability for all involved;
- (ix) Documented interdependencies among SCPs for service delivery, including timing, quality and communications standards as to ensure that handoffs or support requirements between the parties are understood, documented, and followed by all parties;
- (x) Service terms, conditions, operating hours, response times and escalations; and
- (xi) Periodic review and optimization of the OAs based on better practices, lessons learned and DCS Customer feedback. The project team leaders from the Successful Respondent, MSI, and SCPs shall meet regularly, but no less frequently than monthly, during the term of this Agreement, to prioritize tasks, discuss changes and scheduling, identify problems and resolutions, and otherwise coordinate and cooperate in connection with the development and implementation of the Services.

(d) Further, the Successful Respondent will establish Operating Agreements (OA) with both other DCS Service Component Providers and the MSI that the Successful Respondent provides services to, or consumes services from in the overall context of the DCS program as to:

- (i) Provide a holistic Service to DCS Customers inclusive of all work, process, communication, and data/report sharing requirements contained herein;
- (ii) Minimize, and to the greatest extent possible, eliminate, process, and communication gaps or overlaps in Service Request management, ITIL I/P/C processes and Service Delivery processes as to drive a cohesive and well-run Service to DCS customers and DIR; and
- (iii) Ensure participation and success of multi-service provider projects, initiatives, incident and problem resolution within the DCS program where such elements require multi-party participation to deliver a project, resolve an issue or problem, or provide a superior delivery/resolution outcome to DCS customer(s) and/or DIR as required.

- (e) The Successful Respondent will cooperate with DIR in its attempts at transferring, replacing or augmenting the services responsibilities to another provider in a manner in keeping with not adversely affecting the provision of ongoing services and other projects being performed concurrent with this Service.
- (f) Due to the nature of the Shared Technology Services program and the integration of SCPs therein, DIR expects that there may be occasions where an SCP's responsibility may need to be revised to support the overall success of the program and ensure service continuity. DIR therefore retains the sole right to remove and/or reassign a portion of a SCP's scope as necessary. There may also be an occasion where DIR may ask that a SCP absorb work related to their scope of Services in an effort to provide continuity of service to the program where a gap may be discovered or a change for the betterment of the program may be needed. Should either of these actions be needed, the Successful Provider will work with DIR in good faith to execute those changes through the appropriate contract change request process. It is DIR's intent that the Successful Respondent will perform Services within the Shared Technology Services Program such that all actions support success of the program and prevent negative outcomes for Customers as may be anticipated and prevented by the Successful Respondent.

### **3.21. Successful Respondent Cooperation**

- (a) Successful Respondent shall perform the Services in a manner that shall not:
  - (i) disrupt or have an unnecessary adverse impact on the activities or operations of DIR, the DCS Customers, or a DIR Contractor,
  - (ii) degrade the Services then being received by DIR or the DCS Customers, or
  - (iii) disrupt or interfere with the ability of DIR or the DCS Customers to obtain the full benefit of the Services.
- (b) Successful Respondent acknowledges that its provision of the Services shall require significant cooperation with third parties, and Successful Respondent shall fully cooperate and work in good faith with third parties as described in this Agreement and to the extent otherwise requested by DIR. DIR and DCS Customer personnel and DIR Contractors shall comply with Successful Respondent's reasonable security and confidentiality requirements and shall, to the extent performing work on Software, Equipment or Systems for which Successful Respondent has operational responsibility, comply with Successful Respondent's reasonable standards, methodologies, and procedures as communicated in writing to such third parties by Successful Respondent.

### **3.22. Onboarding New Customers**

- (a) Each time a potential new customer requests DCS services, the Successful Respondent will develop a DCS-specific service offering directed towards that potential new Customers of DCS to use DCS service components and elements contained in this Exhibit. This Service offering will be utilized upon the request of DIR as a pre-onboarding service designed to understand and identify all infrastructure related impacts that require addressing by (or through) any one of:
  - (i) The new DCS Customer (or extension of existing DCS Customer's utilization of DCS services);

- (ii) Accommodations or considerations that impact DCS SCPs as they relate to Services in this Exhibit;
  - (iii) Customer environment remediation activities required to align with and leverage DCS standard computing, support and security architectures, constructs, standards and policies; and
  - (iv) Alteration or enhancement of DCS infrastructure environment processes, tools or devices as to incorporate the new DCS Customer into DCS services.
- (b) The Successful Respondent, as a result of such service offering will create a new DCS Customer-specific Service Impact and Optimization Assessment and Remediation Plan that includes:
- (i) Compute and storage service standardization and optimization requirements inclusive of operating systems assets and security provisions as required;
  - (ii) Incorporation of elements required to optimally use Backup/Restore, DR, and Database services as contained herein;
  - (iii) Security optimization and implementation services requirements;
  - (iv) Customer-specific accommodations and considerations;
  - (v) Network name, addressing, services and other factor impacts and remediation requirements as to enable the DCS Network provider's standards;
  - (vi) DCS Implementation and Cutover Plan; and
  - (vii) Detailed roles and responsibilities of DCS SCPs, the Successful Respondent and the new DCS customer as it relates to Services and service elements contained herein.
- (c) Upon written approval to proceed with this onboarding and optimization plan, the Successful Respondent will perform the services contained in this Solution Proposal Package as a project in accordance with the established project management and RFS processes and requirements.

### 3.23. Project Bench

#### 3.23.1. Initial Staffing

- (a) The Successful Respondent shall provide technical staff resources to both solution (architect) and implement DCS Customer and DIR requested projects related to the Services, including, but not limited to, new development solution designs and implementation projects, and upgrades/expansion to existing Services within the timelines provided in Section [3.23.2 Work Specification and Authorization Process](#) for responding to Requests for Solution(s). Transition, Transformation, Operations and Refresh projects are not eligible for the project bench.
- (b) Resources assigned to the bench must meet minimum CJIS security qualifications. All project bench resources must provide services within the continental US.
- (c) Respondent shall define its minimum project bench by skill set and shall describe its solution for meeting DCS Customer demand with prequalified, CJIS background checked staff and for staffing up and down as the DCS Customer project work fluctuates.
- (d) **NOTE:** Multi tower Project Management is performed by the MSI. Successful Respondent should NOT propose project management resources, unless requested to do so by DIR Representative.

### 3.23.2. Work Specification and Authorization Process

- (a) The Successful Respondent will provide services on request as authorized in writing in accordance with the mutually agreeable work estimation, quotation, and approval process. Requests will be made through the MSI Service Catalog via a Request for Solution (RFS), to effectively manage, authorize and report on demand.
- (b) The Respondent will provide a project bench staffing plan that includes resumes for proposed resources as part of its proposal response to this RFO. Proposed resources will be made available to begin work on a solution request within one (1) business day of receipt. Proposed resources will be made available as necessary to meet the solution implementation date established in the solution proposal and agreed by the Customer.
- (c) In the event a proposed resource is not available for any reason, Successful Respondent will provide a replacement resource of equal or better qualifications.

### 3.23.3. Demand Management

The Successful Respondent will identify project resources by skill type and will enter staff availability into the MSI's demand management system. The Successful Respondent will assign those resources to the solution requests and project implementations. The staff will estimate work effort in hours to both solution and implement requests and will track these estimates in the MSI's demand management system. The staff will then track actual hours spent by project in the MSI's demand management system.

### 3.23.4. Demand Management Forecasting and Reporting

- (a) The Successful Respondent will use the MSI demand management resource planning tool to provide a schedule of project hours consumed (by DCS Customer activity, resource type, and Project) to forecast requested projects. The Successful Respondent will use the MSI tool to demonstrate accurate estimating and staff allocation to projects such that deadlines are met. Successful Respondent will also participate in project staffing and resource assignment meetings as requested.
- (b) Two (2) SLAs will report Successful Respondent timeliness and quality of project delivery:

#### 3.23.4.1. Solution Proposal Delivery

TSS will assess the complexity of the solution request and assign an SLA due date, which may be adjusted with sufficient justification by mutual agreement of the Successful Respondent and the customer.

#### 3.23.4.2. Solution Implementation

TSS will establish the solution implementation deadline based on the MSI's demand management resource planning tool and on the Successful Respondent's estimated scope and proposed implementation date. This implementation date may be adjusted with sufficient justification by mutual agreement of the Successful Respondent and the customer.

### 3.23.5. Review of Uses, Adjustment of Project Bench, and Resource Verification

The Successful Respondent and DIR will meet semi-annually to review the existing minimum bench and adjust as required. In the event DIR determines the minimum bench requires adjustment, DIR and the Successful Respondent will work to establish a monthly number of hours and base staffing level commitment for each year of the agreement.

### 3.24. Enterprise SaaS Services

In addition to Services as defined in Section 3.1.1 Software as a Service (SaaS) / Platform as a Service (PaaS) Purchases on Behalf of Customer, Successful Respondent shall provide ongoing support services for Enterprise SaaS solutions. These Enterprise SaaS products currently include Salesforce and Texas Imagery (using Google Global Imagery Services). The Successful Respondent shall be responsible for the delivery of services including:

- (i) Support DCS Customer in Submit request in Service Catalog;
- (ii) Assist DCS Customer in creating tickets and ensuring assignment to Software Procurement personnel;
- (iii) Provide design and integration support based upon request;
- (iv) Request quote from Enterprise SaaS provider;
- (v) Review quote from Enterprise SaaS provider;
- (vi) Execute Purchase Order process for approvals and assurance;
- (vii) Issue Purchase Order to Enterprise SaaS provider;
- (viii) Create Contract billing record;
- (ix) Close out software procurement ticket;
- (x) Provide billing detail to MSI;
- (xi) Track and renew software contracts;
- (xii) Monitor and report Service Level achievement;
- (xiii) Support incidents, outages and performance issues with Enterprise provider;
- (xiv) Support DCS Customer, MSI and other SCP with events, issues and incidents related to Enterprise SaaS services.

## 4. Steady State Service Evolution and Optimization Services

### 4.1. Environment Review and Advisory Services

The Successful Respondent will support DIR, TSS and the MSI in the administration, implementation, optimization, and support of the use of the Service and service elements inclusive of all hardware, products, services, devices, tools, operational processes and emerging standards as to support DCS' position with respect to high performance, high quality, and high availability (to the extent contained and as applicable to the work in this Exhibit) Service infrastructure provided by the Successful Respondent in the performance of the contracted responsibilities under this Exhibit.

## 4.2. Service Capacity Planning

- (a) The Successful Respondent will support DIR, TSS and the MSI capacity planning exercises through service review meetings and, if requested due to an unforeseen requirement, participation in a required number of ad-hoc reviews coincident with these new requirements and service needs to correctly plan for capacity – periodic capacity increases as well as burst requirements. To support this planning and review process, the Successful Respondent will monitor system use, forecast capacity, and then review with the MSI and DCS service providers as applicable on a quarterly basis to share growth, concerns, and information with the DCS community to inform investments and projects DIR, DCS providers, the MSI, or DCS Customers may need to undertake.
- (b) As part of these responsibilities, the Successful Respondent will support the MSI by:
  - (i) Identify future consumption trends and capacity requirements in conjunction with provided capacity usage reports, suggest new projects or efforts as it pertains to the Services;
  - (ii) Review supported scope compute, storage and Service performance and throughput for new applications and DCS Customer deployments before promotion into the production.

## 4.3. Technology Planning and Optimization Roadmap

- (a) The Successful Respondent will support TSS and the MSI in written annual review of a multi-year Service roadmap inclusive of all projects, optimization and transformation initiatives. This review will be designed to ensure that the ongoing use of DCS supports future deployments, stabilization and extensions into new lines of business and DCS Customer groups. Additionally, this review will highlight related State-wide and DCS Customer change initiatives and identified opportunities to leverage DCS in support of the State’s mission.
- (b) The Technology Plan and Roadmap is an annual Critical Deliverable but will require quarterly updates.
- (c) The Successful Respondent will implement the optimization and technology improvements identified in the plan and approved by DIR.

### 4.3.1. Technology Planning Process

- (a) The Successful Respondent shall adhere to the TSS and MSI process and ongoing program management for the establishment, currency, tracking, and publishing of a Technology Plan that incorporates input from DIR, TSS, MSI, DCS Customers, and SCPs and aligns with the governance processes. The Technology Planning Process is typically based on annual deliverables. However, due to the high pace of change and velocity of potential movement to the Public Cloud, these deliverables need to be reviewed and updated on a quarterly basis.
- (b) This plan will include, but not limited to:
  - (i) Introduction of new services, products, offerings, technologies, capabilities, and processes to drive more efficient and secure operations and DCS Customer experiences in the Public Cloud;

- (ii) Ongoing evaluation and execution of Proof of Concepts to ensure new capabilities are aligned with DCS program objectives and communicated following the enterprise roadmaps in working with TSS.
- (iii) Migrate systems and services from DCS legacy environments and DCS Customer locations;
- (iv) Implementation of new Service features and functions including wider deployment and use of DCS services, and extend the safe, secure, and available nature of DCS services to all DCS Customers and DCS Prospects;
- (v) Retirement of legacy Service elements and platforms where DCS provides similar or superior functional/technical footprints;
- (vi) The automation of manual tasks associated with the Services including leading in the identification, solutioning and planning of MSI and/or Successful Respondent automation opportunities to increase automation, efficiencies and value;
- (vii) Proactively identify strategies and approaches for future IT delivery that Successful Respondent believes will provide DIR and DCS Customers with competitive advantages and that may result in increased efficiency, performance, or cost savings; and
- (viii) Evaluate market technology advances for Successful Respondent's tools and technologies that may provide DIR and DCS Customers greater capabilities, performance improvements or improve Service Levels of the DCS environment. Tool selection will be in accordance with DIR and DCS Customers' standards and technical architectures.

#### 4.3.2. Processes, Procedures, Architecture, Standards, and Planning.

- (a) As requested by DIR, Successful Respondent, without limiting the obligation of the Parties under **MSA Section 8.11 Compliance with Laws**, shall assist DIR and the appropriate governance committee (as specified in Article [8 DCS Governance Model](#)), on an on-going basis in defining:
  - (i) the standards, policies, practices, processes, procedures and controls to be adhered to and enforced by Successful Respondent in the performance of the Services, including those identified herein, and
  - (ii) the associated IT technologies architectures, standards, products and systems to be provided, operated, managed, supported and/or used by Successful Respondent in connection therewith (collectively, the "DIR Standards").
- (b) The Parties acknowledge and agree that, as of the Commencement Date, Successful Respondent is fully informed as to the DIR Standards that have been communicated to it in a manner consistent with **MSA Section 4.4 DIR Rules/Employee Safety**.
- (c) Successful Respondent also shall assist DIR on an annual basis in preparing Technology Plans that include both long-term strategic and short-term implementation plans. The assistance to be provided by Successful Respondent shall include:
  - (i) active participation with DIR and the appropriate governance (as specified in in Article 8 [DCS Governance Model](#)), addressing such issues;;
  - (ii) assessments of the then-current DIR Standards at a level of detail sufficient to permit DIR to make informed business decisions;
  - (iii) analyses of the appropriate direction for such DIR Standards;
  - (iv) the provision of information to DIR regarding Successful Respondent's technology strategies for its own business;

- (v) recommendations regarding standards, processes, procedures and controls and associated technology architectures, standards, products and systems; and
  - (vi) the provision of current, historical, and forecasted system capacity, performance and utilization metrics at reasonable requested levels of detail.
- (d) With respect to each recommendation, Successful Respondent shall provide the following at a level of detail sufficient to permit DIR to make an informed business decision:
- (i) the projected cost to DIR and the DCS Customers and cost/benefit analyses;
  - (ii) the changes, if any, in the personnel and other resources Successful Respondent, DIR and/or the DCS Customers shall require to operate and support the changed environment;
  - (iii) the resulting impact on the total costs of DIR and the DCS Customers;
  - (iv) the expected performance, quality, responsiveness, efficiency, reliability, security risks, and other service levels; and
  - (v) general plans and projected time schedules for development and implementation. Any assistance provided by Successful Respondent under this Section shall be at no additional fee or charge beyond the Charges specified in **Exhibit 2 Pricing** for the Services, unless an additional Charge has been approved by DIR.
- (e) DIR shall have final authority to promulgate DIR Standards and Strategic Plans and to modify or grant waivers from such DIR Standards and Strategic Plans. Successful Respondent shall:
- (i) comply with and implement the DIR Standards and Strategic Plans in providing the Services,
  - (ii) work with DIR to enforce the DIR Standards and Strategic Plans,
  - (iii) modify the Services as and to the extent necessary and on a schedule to conform to such DIR Standards and Strategic Plans, and
  - (iv) obtain DIR's prior written approval for any deviations from such DIR Standards and Strategic Plans.

### 4.3.3. Software Currency Requirements

#### 4.3.3.1. Currency of Software

Subject to and in accordance with **Exhibit 2 Pricing, Attachment 2.1 Financial Responsibility Matrix**, Successful Respondent shall maintain reasonable currency for Software for which it is financially responsible under this Agreement and provide maintenance and support for Software (including new Upgrades, Major Releases, and Minor Releases) for which it is operationally responsible under this Agreement. At DIR's direction, Successful Respondent shall operate, maintain and support multiple releases or versions of the same Software without any increase in the Monthly Base Charge. In addition, unless otherwise directed by DIR, Successful Respondent shall keep Software within release levels supported by the appropriate third-party vendor to maintain compatibility with other Software or Equipment components of the Systems and of DIR's Retained Systems and Processes. To the extent Third Party Software for which Successful Respondent is operationally responsible under this Agreement is no longer supported by the applicable licensor or manufacturer, Successful Respondent shall use commercially reasonable efforts to perform maintenance for such Software as required. For purposes of this Section, "**reasonable currency**" means that, unless otherwise directed by DIR:

- (i) Successful Respondent shall maintain Software within one (1) Major Release of the then-current Major Release, unless otherwise specified pursuant to the Software Currency guidelines set out in **Exhibit 2 Pricing, Attachment 2.2 Financial Responsibility Matrix** and
- (ii) Successful Respondent shall install Minor Releases promptly or, if earlier, as requested by DIR.

#### 4.3.3.2. Evaluation and Testing

- (a) Prior to installing a new Upgrade, Major Release, or Minor Release, Successful Respondent shall evaluate and test such Software to verify that it shall perform in accordance with this Agreement and the DIR Standards and that it shall not:
  - (i) increase DIR's or the DCS Customers' total cost of receiving the Services,
  - (ii) have an adverse impact on performance or require changes as described in Section [4.3.3.3 Updates by DIR](#), or
  - (iii) violate or be inconsistent with DIR Standards, DCS Technology Plans, or applicable Laws.
- (b) The evaluation and testing performed by Successful Respondent shall be at least consistent with the reasonable and accepted industry norms applicable to the performance of such Services and shall be at least as rigorous and comprehensive as the evaluation and testing usually performed by highly qualified SCPs under such circumstances.

#### 4.3.3.3. Updates by DIR

DIR and the DCS Customers have the right, but not the obligation, to install new Upgrades, Major Releases or Minor Releases, replace or otherwise make any other changes to Software for which DIR is financially responsible under this Agreement.

#### 4.3.3.4. Approval by DIR or DCS Customer

- (a) Successful Respondent shall seek approval from either DIR or the DCS Customer with control over the relevant software prior to installing any new Upgrade, Major Release or Minor Release. Successful Respondent shall provide DIR or DCS Customer with the results of its testing and evaluation of such Software and a detailed implementation plan and shall not install such Software if directed not to do so by DIR or DCS Customer. Where specified by DIR, Successful Respondent shall not install new Upgrades, Major Releases or Minor Releases or make other Software changes until DIR has completed and provided formal signoff on successful user acceptance testing. Successful Respondent shall not install new Upgrades, Major Releases or Minor Releases or make other Software changes if doing so would require DIR or the DCS Customers to install new releases of, replace or make any other changes to any Software for which DIR or DCS Customer is financially responsible under this Agreement unless DIR or DCS Customer consents to such change in advance.
- (b) If DIR rejects Successful Respondent's proposed Upgrade or replacement of a Software version that is back-leveled such that it is no longer supported by the applicable Software manufacturer, Successful Respondent may be relieved from applicable Service Levels in accordance with **MSA Section 5.2 Savings Clause**.

- (c) Notwithstanding the other provisions of Section [4.3.3 Software Currency Requirements](#), if DIR rejects Successful Respondent's proposed Upgrade or replacement of a Software version that is back-leveled such that it is no longer supported by the applicable Software manufacturer and Successful Respondent is thereafter required to incur additional fees and expenses to obtain necessary maintenance for such Software version from such Software manufacturer in order to meet its obligations under this Agreement, DIR shall reimburse Successful Respondent for the reasonable fees and expenses thus incurred, but only if:
- (i) Successful Respondent is unable, using commercially reasonable efforts, to perform such maintenance using Successful Respondent Personnel, including maintenance of knowledge among Successful Respondent Personnel about Software versions retained or desired to be retained by end users,
  - (ii) DIR has rejected Successful Respondent's proposed Upgrade or replacement of such Software version after being notified by Successful Respondent that it will not be able to provide certain required maintenance for such Software version using Successful Respondent Personnel,
  - (iii) Successful Respondent notifies DIR of its intent to use such Software manufacturer to perform maintenance and the anticipated fees and expenses associated therewith and obtains DIR's approval prior to incurring such fees and expenses, and
  - (iv) Successful Respondent uses commercially reasonable efforts to minimize the fees and expenses to be reimbursed by DIR.

#### 4.3.4. Software Currency Management

Successful Respondent's responsibilities include:

- (i) Automated monitoring currency of hardware and software relative to respective vendor sources resident in each Successful Respondent's technology plan and ensure proper notification is provided to DIR, DCS Customer, and Third-Party Vendors regarding support and software currency plans.
- (ii) 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).
- (iii) As directed by DIR, also support releases as specified in the Financial Responsibility Matrix.
- (iv) Support Software that is no longer supported by the Third-Party Vendor.
- (v) Provide support for all Software versions and release levels that exist as of the Effective Date until otherwise directed by DIR.
- (vi) Provide monthly reports of upcoming software releases, software renewals and end-of-support notices on affected DCS Customers to the MSI, at least 180 days prior to expiration date.

#### 4.3.5. Technology Adoption and Alignment

The Successful Respondent will provide information in the format required by the MSI to:

- (i) Develop and structure the plan as to coordinate the aggregation of technical planning information from DIR, DCS Customers, Successful Respondent, and SCPs as directed by DIR and include an implementation roadmap, consistent with DIR's business roadmap with estimated timing, in alignment with the Technology Plan, for DIR and DCS Customers; and
- (ii) Provide linkage with technology currency requirements that align with technology refresh plans (e.g., software version migrations) and include input from DIR to identify candidates and

requirements for the deployment of new technology or the automation of tasks associated with the Services and/or DIR's and DCS Customers' business processes.

#### 4.3.6. Technology Standards

The Successful Respondent will research and recommend standard products to the Technology Solution Services (TSS) for adoption into the program.

- (i) Publish and make available the description of services and offerings by Provider that are in use on a quarterly basis
  - (ii) Publish and make available the description of Standard Products to Authorized Users as requested by DIR;
  - (iii) Provide standards for supporting open source software;
  - (iv) Make the description of approved services and offerings available on the MSI portal;
  - (v) Align the approved services and offerings list with DIR's strategic direction, and technical architecture;
  - (vi) Provide mechanisms and processes to capture feedback and business needs from DCS Customers as to potential changes required in approved services and offerings;
  - (vii) Publish service and offering evaluations to help DCS customers understand potential use cases and value expected; and
  - (viii) Maintain all products in use as of Commencement and provide expertise for new standard services and offerings as they are added to the program.
- 

#### 4.4. Annual Review of Service Roadmap

- (a) In conjunction with regularly scheduled operational meetings with DIR Personnel or a meeting of DCS Governance, and in driving continuous improvement requirements of this Exhibit, the Successful Respondent at least annually will sponsor a meeting to review recent or anticipated industry trends, emerging technologies, technology advancements, alternative processing approaches, new tools, methodologies or business processes (collectively "best practices") that, at DIR's choosing, could optimize the cost, efficiency, computing capacity, server density or otherwise drive efficiencies for both DCS Customers and the Successful Respondent.
- (b) **NOTE:** See **Attachment 1.1 Deliverables** for specific information regarding due dates, timelines, etc.
- (c) Throughout the Term, Successful Respondent shall:
  - (i) identify and apply best practice techniques, methods, and technologies in the performance of the Services;
  - (ii) train Successful Respondent-Personnel in the use of new techniques, methods, and technologies that are in general use within Successful Respondent's organization and the IT and business consulting industries; and
  - (iii) make necessary investments to keep and maintain the Software and other assets used to deliver the Services at the level of currency defined in this Section.

## 4.5. Public Cloud and Computing Optimization Services

### 4.5.1. Physical and Virtual Asset Usage Optimization Services

- (i) The Successful respondent will assist the TSS, MSI and the Texas Private Cloud SCP to assess the utilization of all assets (computing platforms, servers, storage, network interface points and the like) to:
- (ii) Utilize Public Cloud methods and expertise and apply “public cloud” techniques to the DCS Private Cloud environment including technology optimization, “standardization as a service”, and collaborative solutioning with DCS Customers to reduce complexity and drive higher levels of value and lower unit costs by service element; and

### 4.5.2. Service Standardization and Optimization Services

The following elements are required to drive the overall consistency, repeatability and reliability of the Service:

- (i) Simplification of service offerings and support tiers to move the Service to a more consistent support model (e.g., 24x7) that drives higher levels of consistency and reliability;
- (ii) Drive initial quality in service element implementations (e.g., “right first time”) and reduce I/P/C service requests wherever possible through implementation of repeatable templates, automation and utilization of programmatic orchestration that is aligned and leverages software defined data center techniques (and software defined networking as provided by the Managed DCS Network SCP);
- (iii) Review of all DCS Customer-facing (and MSI-supporting) help channels and service reports to eliminate extraneous and conflicting elements including removing “manual steps through the automation of I/P/C communications and processes;
- (iv) Identify and eliminate recurring problems in the environment through streaming and automation of environment monitoring and alerts;
- (v) Via tools and automation, create a single view of the enterprise – production/non-production and private/public cloud to enhance DCS Customer experience, for operations and maintenance, and risk management/security capabilities;
- (vi) Implement automated software tracking in all environments to ensure currency, licensing, patching, support, and exposure to vulnerabilities;
- (vii) Implement context-specific technical guides and on-screen help that extend the native public cloud provider capabilities;
- (viii) Automate patch management around standards (O/S, tools and support models) wherever possible to remove incompatibilities and “exception” patching that could result in leaving DCS Customer environments either unpatched, non-contemporary or unsupported by OEM software; and
- (ix) Automate data collection to drive better data and more timely data collection to facilitate Service decision making, cross functional coordination and long-term planning.

#### 4.5.3. Storage Optimization Services

From a storage perspective, the Successful Respondent will assist the TSS, MSI and the Texas Private Cloud SCP to:

- (i) Consolidate storage management to migrate the environment to use of Public Cloud storage as opposed to “on premise” storage on servers and manage DCS storage consistently regardless of workload hosting location, as opposed to environment-specific items;
- (ii) As part of this element of the Service, the Successful Respondent will ensure that the corresponding backup/restore environment and disaster recovery capabilities are in no way diminished, and are improved through the implementation of enterprise class storage management, replication, and data protection methods;
- (iii) Continuously improve the tracking of location(s) of sensitive and restricted data sets and files so that DCS Customers are always apprised of the state of their data in an accurate and programmatic method.

#### 4.5.4. Middleware Optimization Services

The Successful Respondent will, for the Middleware service elements of the overall Service:

- (i) “Unbundle” middleware from standard offerings where it is not required by the DCS Customer and move to an “a la carte” service based on actual DCS Customer need and use from a transactional and file exchange perspective;
- (ii) Provide guidance by way of standards and integration guides so that DIR may include integration requirements in all future DIR systems that are oriented to consuming DCS Services as requirements to utilize standard integration service and tools offered in the middleware elements of the Service.

#### 4.5.5. Software Licensing and Tracking Services

The Successful Respondent will, for all service elements of the Service:

- (i) Track and monitor the consumption of all DCS standard software titles that comprise the Service and identify opportunities to better align (with DIR support) license models to actual DCS Customer consumption patterns and requirements; and
- (ii) Identify application level software titles, including versioning and patch levels, as a service to DCS and as to assist DCS Customers in understanding potential vulnerable titles with respect to security threat vectors, as well as obsolete and unsupported titles.

#### 4.5.6. Security Optimization and Implementation Services

To enable DCS to drive higher levels of compliance and defense with respect to its security posture within the overall Service, the Successful Respondent will (for non-compliant elements):

- (i) Follow DIR policy, industry standards and best practices in tooling and processes associated with provisioning, Service integration and management, DIR inter-connection with public cloud elements and implementation of public cloud computing;
- (ii) Ensure that all components are monitored actively for security vulnerabilities, flaws, virus/malware, and other elements that would undermine the security posture of DCS;
- (iii) Drive higher levels of data encryption across all elements of the service for data in flight and at rest – particularly for those service elements that are prone to attack or include high numbers of records with sensitive data;
- (iv) Seek opportunities to implement identity management, multi-factor authentication and leverage DCS programmatic fraud/intrusion detection for all trusted userids (e.g., root, admin, dba) within the scope of Services; and
- (v) Support regular third-party penetration testing of all DCS public cloud assets and remediate all issues within the Service.

#### 4.5.7. Database Optimization and Implementation Services

The Successful Respondent will, for the database service elements of the overall Service:

- (i) Drive to commodity, engineered solution, and managed public database cloud database solutions when instances that support database are due for technical refresh and ensure that the performance, value and cost attributes of the database align with demonstrated needs of DCS Customers and their applications;
- (ii) Seek opportunities to minimize database software licensing and maintenance from OEMs through moving to licensing models that better reflect DCS Customers’ current needs while ensuring that software licensing compliance is maintained; and
- (iii) Position to adopt No-SQL and New-SQL databases for next generation business models (e.g., spatial, data analytics, blockchain) as required by DCS Customers.

#### 4.5.8. Backup/Restore Optimization and Solutioning Services

The Successful Respondent will, for the backup/restore and data protection service elements of the overall Service:

- (i) Coordinate with and assist MSI, TSS SCP and TPC SCP to establish a schedule for DCS Customers to use a single backup/recovery standard for all storage (data center, local and cloud) that includes on-premise (virtual tape), off-premise and cloud-based backups as appropriate to the DCS Customer environment including database and file system snapshots, replication, and disaster recovery capabilities from public cloud providers;
- (ii) Where the economics and data protection model are appropriate, utilize public cloud archival storage for backup/archive of data (if allowed by Texas state law) – particularly those that are archival and non-volatile from an operational or transactional perspective (e.g., reference, cold storage, long-term backups, etc.);
- (iii) Support DIR in “selling” backup/recovery services to DCS Prospects and higher ed as a risk mitigation service and an entry point into DCS;

- (iv) Drive higher levels of end-to-end encryption of backup data regardless of media/target to ensure that DIR data is always protected; and
- (v) Assist service evolution elements that include the use of containerization techniques to migrate DCS Customer workloads, configuration and data within the DCS private cloud and (as appropriate) to public cloud providers.

## 5. Successful Respondent Personnel Requirements

**NOTE:** all roles (DIR minimum or otherwise) must be included in the Respondent Staffing Plan as required in this Section. For all DIR roles marked “as required” Respondents are to include (within their proposal) the staffing level required of DIR to ensure that the Successful Respondent project is staffed adequately.

### 5.1. Key Personnel Staffing

#### 5.1.1. Approval of Key Personnel

The positions designated by DIR to be filled by Key Personnel and the Key Personnel that have been selected and approved by DIR as of the Effective Date are identified in Attachment 1.5 Key Personnel. At least thirty (30) days prior to assigning an individual to act as one (1) of the Key Personnel, whether as an initial assignment or a subsequent assignment, Successful Respondent shall notify DIR of the proposed assignment, shall introduce the individual to appropriate DIR representatives, shall provide reasonable opportunity for DIR representatives to interview the individual and shall provide DIR with a resume and such other information about the individual as may be requested by DIR. If DIR in good faith objects to the proposed assignment, the Parties shall attempt to resolve DIR's concerns on a mutually agreeable basis. If the Parties have not been able to resolve DIR's concerns within five (5) DIR Business Days of DIR communicating its concerns, Successful Respondent shall not assign the individual to that position and shall propose to DIR the assignment of another individual of suitable ability and qualifications. DIR may add, delete, or otherwise change the positions to be filled by Key Personnel under this Agreement.

#### 5.1.2. Continuity of Key Personnel

- (a) Successful Respondent shall cause each of the Key Personnel initially assigned at execution to devote full time effort to the provision of Services under this Agreement for, at a minimum, twenty-four (24) months post Commencement. Successful Respondent shall cause each subsequent assignment of Key Personnel to devote full time effort to the provision of Services for, at a minimum, the applicable period specified by the Successful Respondent at the time of subsequent assignment, from the date he or she assumes the position in question (provided that, in the case of Key Personnel assigned prior to the Commencement Date, the minimum period shall be measured from the Commencement Date). Successful Respondent shall not transfer, reassign or remove any of the Key Personnel (except as a result of voluntary resignation, involuntary termination for cause, illness, disability, or death) or announce its intention to do so during the minimum period without DIR's prior approval, which DIR may withhold in its reasonable discretion based on its own

self-interest. In the event of the voluntary resignation, involuntary termination for cause, illness, disability or death of one (1) of its Key Personnel during or after the specified period, Successful Respondent shall:

- (i) give DIR as much notice as reasonably possible of such development, and
  - (ii) expeditiously identify and obtain DIR's approval of a suitable replacement.
- (b) In addition, even after the initial twenty-four (24) month assignment period, Successful Respondent shall transfer, reassign, or remove one (1) of its Key Personnel only after:
- (i) giving DIR at least thirty (30) days prior notice of such action (except to the extent such removal involves termination due to cause or performance as defined below),
  - (ii) identifying and obtaining DIR's approval of a suitable replacement at least thirty (30) days prior to such transfer, reassignment, or removal,
  - (iii) providing DIR with a plan describing the steps and training (including knowledge transfer) that Successful Respondent shall perform to transition responsibility to the replacement, and
  - (iv) demonstrating to DIR's satisfaction that such action shall not have an adverse impact on Successful Respondent's performance of its obligations under this Agreement.
- (c) Unless otherwise agreed, Successful Respondent shall not transfer, reassign, or remove more than one (1) of the Key Personnel in any six (6) month period; provided, however, the foregoing shall not prevent Successful Respondent from terminating a Key Personnel for cause or performance as defined below.
- (d) For purposes of this Section cause means disregard of Successful Respondent's rules, insubordination, or misconduct (as defined in Successful Respondent's human resource policies), or criminal conduct, and performance means that the individual's job performance is at a level that would justify dismissal under Successful Respondent's human resources policies.

### 5.1.3.Retention and Succession

Successful Respondent shall implement and maintain a retention strategy designed to retain Key Personnel on DIR's and the DCS Customers' accounts for the prescribed period, such as retention bonuses. Successful Respondent shall also maintain active succession plans for each of the Key Personnel positions.

### 5.1.4.Successful Respondent Account Director.

Successful Respondent shall designate a "**Successful Respondent Account Director**" who, unless otherwise agreed by DIR, shall maintain his or her office in Austin, Texas. The Successful Respondent Account Director shall:

- (i) be one (1) of the Key Personnel;
- (ii) be a full time employee of the Successful Respondent;
- (iii) devote his or her full time and effort to managing the Services;
- (iv) remain in this position for a minimum period of two (2) years from the initial assignment (except as a result of voluntary resignation, involuntary termination for cause, illness, disability, or death);
- (v) serve as the single point of accountability for the Services;

- (vi) be the single point of contact to whom all DIR communications concerning this Agreement may be addressed;
- (vii) have authority to act on behalf of Successful Respondent in all day-to-day matters pertaining to this Agreement;
- (viii) have day-to-day responsibility for service delivery, billing and relationship management; and
- (ix) have day-to-day responsibility for ensuring customer satisfaction and attainment of all Service Levels.

## 5.2. Key Service Personnel Positions

- (a) In an effort to foster a mutually supportive and collaborative environment in which the Services are provided in an effective manner that drives value to DCS Customers, the Parties will jointly review certain Key Successful Respondent Management and DIR or DCS Customer-facing positions (collectively “Key Personnel”), including the Successful Respondent Account Representative. “Key Personnel” will include the following at a minimum:
  - (i) Account Director with overall contract, financial and service delivery accountability for the contract. This position shall have decision making authority for all aspects of the contract. The Account Director shall be dedicated full time to the Successful Respondent’s contract, not leveraged to other accounts.
  - (ii) Service Delivery Director with overall accountability for delivery of the Successful Respondent’s requirements. The Service Delivery Director shall be dedicated full time to the Successful Respondent’s contract, not leveraged to other accounts.
  - (iii) Financial Director with overall accountability for all chargeback, invoicing, billing disputes, pricing, and financial reporting.
  - (iv) Technical Director with overall accountability for technology planning, optimization, and innovation.
  - (v) Transition Director with overall accountability for delivery of the Successful Respondent’s contract transition from contract execution through Commencement of services, and through completion and DIR acceptance of all Transition deliverables.
  - (vi) Security Director with overall accountability for security policies, procedures, planning, evaluation and technology.
  - (vii) Cloud Service Delivery Manager with overall accountability for all cloud technologies and services.
  - (viii) Other, as the Successful Respondent deems key to the fulfillment of its contract obligations.
- (b) Key Personnel shall be committed for twenty-four (24) months minimum from contract execution unless stated otherwise. After twenty-four (24) months, replacement Key Personnel shall be committed for a minimum of twelve (12) months.
- (c) The Successful Respondent shall provide a table with information on Key Personnel, including name, title, functional area, percentage dedicated and commitment timeframe. The table shall be maintained by the Successful Respondent and provided to DIR upon request.
- (d) Based on DIR’s experience with DCS and similar managed services relationships with a variety of leading vendors, DIR feels strongly that the Successful Respondent team (as a team and as individuals) should be regularly reviewed regarding several key factors including, but not limited to:
  - (i) Enablement of DCS initiatives including DCS Customer and DCS Prospect adoption of the DCS program and infrastructure consolidation/standardization initiatives;

- (ii) Attainment of high customer satisfaction in Stakeholder (i.e., DCS Customers, DIR, Service Governance and DCS SCPs) communities and, by extension, importantly end-user communities;
  - (iii) Creation of a highly integrated, collaborative, and mutually supportive delivery of Services under this Exhibit to DIR through the formation of an “integrated team” culture;
  - (iv) Adoption, implementation, and refinement of a “State First” operating culture that is designed to drive value through the relationship and result in a high-performance working partnership between DIR, DCS Customers and Successful Respondent;
  - (v) Incorporation of industry-leading and Successful Respondent best practices in the construction, operation, maintenance and support of DCS while seeking opportunities for continuous refinement and improvement of areas that are directly within the Successful Respondent’s scope, those areas where the Successful Respondent has a reliance on DCS Customers and third parties, and areas in the common interest of driving Service efficiency, quality and timeliness (e.g., value).
- (e) The Successful Respondent, based on then current requirements, DIR preferences and strategies will assess its delivery team in light of DIR’s direction and replace personnel as to align with the then current DIR standards, strategies and evolution roadmap of the in-scope Services within DCS. The Successful Respondent will ensure that the skills, experience, training and certification levels required to perform the Service, within the contracted service levels and volumes are contemporary with DCS Customer need and actively manage - through training, replacement, organizational design and components or other means - as to ensure that its personnel achieve DIR requirements.

### 5.3. Staffing Requirements

#### 5.3.1. Staffing Matrix/Model

- (a) Respondents shall provide a Staffing Plan including the following information:
- (i) An organizational chart including any proposed subcontractors and key management and administrative personnel. All personnel identified as Key Personnel should be identified as part of the organizational chart. The organization chart must identify clear lines of authority and accountability within the organization;
  - (ii) A contingency plan that shows the ability to add more staff, if needed, to meet the Project’s due date(s);
  - (iii) The number of people on site at the CDCs or other facilities at any given time;
  - (iv) A statement and a chart that clearly indicates the time commitment of the Respondent’s Key Project Personnel;
- (b) Respondent must include a statement indicating to what extent, if any, key personnel may work on other projects or assignments that are not related to the Services, during the term of the Contract. DIR may reject any Response that commits the proposed Project Manager or any proposed Project Key Personnel to other projects during the term of the Project, if DIR believes that any such commitment may be detrimental to the Respondent’s performance.
- (c) DIR reserves the right to identify certain roles proposed by the Successful Respondent as Key Personnel in addition to the Key Personnel that the Successful Respondent identifies.

### 5.3.2.Ongoing Staff Service Training

- (a) The Successful Respondent will design and provide DIR with a formal Knowledge Transfer and Education Service in connection with any new service or new technology of the Successful Respondent's service.

Successful Respondent shall:

- (i) Educate and train its operational staff in the use its tools and processes; where appropriate. Successful Respondent shall provide this training to MSI and other SCP staff as required by DIR.
  - (ii) Create handover documentation, training, diagnostic scripts, and operational procedures for operations groups for all Services.
  - (iii) Provide operational training and documentation for support of Services to Respondent's staff, MSI staff, other SCP staff, DIR, and DCS Customers.
  - (iv) Conduct informal information sharing and knowledge transfer services concurrent with the implementation of any Service implementation or release. This knowledge transfer will ensure DCS Customer personnel assigned to support, develop, manage, or operate the Service platform are apprised of the contents of each release, features, functions, known defects and workarounds, and other information to manage and communicate to DIR and DCS Customer leadership (in general) and business stakeholders of the system and DCS Customer functional leaders (specifically) the most effective use of the then current system assets (i.e., the Service element(s), platform(s) and DCS Customer-developed enhancements or extensions).
  - (v) Develop materials such as Frequently Asked Questions (FAQs), one-pagers, how-to documents, or other help pages explaining the use of Services, as required. Materials shall comply with MSI publishing requirements as the MSI will publish these materials on its portal.
  - (vi) In an SMM, document the process workflow sufficient for the MSI and other SCP system staff to support the use of Successful Respondent's systems and Services to perform operational tasks, including, but not limited to the following tasks: simple configuration updates; moderate configuration updates; systems administration activities; and batch processing.
- (b) Concurrently with any DCS Customer production implementation, the Successful Respondent will work with the MSI to develop knowledge articles that highlight specific system support processes, workflows, job aids, and updates arising from the solution implementation.

### 5.3.3.DCS Customer Training

The Successful Respondent will participate in MSI provided training as directed and support the MSI with training delivery for the Service (in general) and operational aspects of the service elements as to enable their use by DCS Customers. The MSI will determine the extent of Successful Respondent involvement in training delivery in addition to the minimum requirements below. As part of this activity area, the Successful Respondent will:

- (i) Work with the MSI in the development, documentation, and delivery of workshops sufficient to prepare trainers and expert users for course delivery by focusing on the process and technical aspects of the training curriculum, including adult learning principles and facilitation techniques
- (ii) Develop an approach and plan for DCS Customer support by:
  - A. Assisting the MSI in establishing a plan to manage the escalation of questions from training sessions and the communication of answers back out to trainers; and
  - B. Working with the MSI to develop an approach and plan for communicating with and training DIR stakeholders and vendors on the implemented modules and new business processes.

## 5.4. Replacement, Qualifications, and Retention of Successful Respondent Personnel.

### 5.4.1. Sufficiency and Suitability of Personnel

As a material obligation hereunder, Successful Respondent shall assign (or cause to be assigned) sufficient numbers of Successful Respondent Personnel to perform the Services in accordance with this Agreement (including applicable Service Levels), and such Successful Respondent Personnel shall possess suitable competence, ability and qualifications and shall be properly educated and trained for the Services they are to perform. Successful Respondent will maintain the organizational and administrative capacity and capabilities to carry out all Successful Respondent duties and responsibilities, including providing and supporting the Services, under this Agreement. Notwithstanding transfer or turnover of its personnel, or of its agents' or Subcontractors' personnel, Successful Respondent remains obligated to perform all duties and responsibilities, including providing and supporting the Services, without degradation and in accordance with the terms of this Agreement.

### 5.4.2. Responsibility for Successful Respondent Personnel

- (a) Successful Respondent agrees that anyone used by Successful Respondent to fulfill the terms of this Agreement is an employee, agent or Subcontractor of Successful Respondent and remains under Successful Respondent's sole direction and control. In addition, Successful Respondent hereby agrees to be responsible for the following with respect to its employees, agents or Subcontractors:
- (i) damages incurred by Successful Respondent Personnel or Subcontractors within the scope of their duties under this Agreement; and
  - (ii) determination of the hours to be worked and the duties to be performed by Successful Respondent Personnel or Subcontractors.
- (b) Successful Respondent agrees and will inform its employees, agents, and Subcontractors that there is no right of action against DIR or any DCS Customer for any duty owed by Successful Respondent pursuant to this Agreement. Successful Respondent expressly agrees that neither DIR nor any DCS Customer assumes any liability for the actions of, or judgments rendered against, the Successful Respondent, its employees, agents, or Subcontractors. DIR's liability to the Successful Respondent's employees, agents, and Subcontractors, if any, will be governed by Chapter 101, Texas Civil Practice & Remedies Code.

### 5.4.3. Requested Replacement

In the event that DIR determines that the continued assignment of any individual Successful Respondent Personnel (including Key Personnel) to the performance of the Services is not in the best interests of any DCS Customer, then DIR may give Successful Respondent notice to that effect requesting that such Successful Respondent Personnel be replaced. Successful Respondent shall have ten (10) DIR Business Days following DIR's request for removal of such Successful Respondent Personnel in which to investigate the matters forming the basis of such request, correct any deficient performance, and provide DIR with assurances that such deficient performance shall not recur (provided that, if requested to do so by DIR, Successful Respondent shall immediately remove (or cause to be removed) the individual in question from all DIR Facilities pending

**State of Texas** Department of Information Resources, Data Center Services

completion of Successful Respondent's investigation and discussions with DIR). If, following such ten (10) DIR Business Day period, DIR is not satisfied with the results of Successful Respondent's efforts to correct the deficient performance and/or to prevent its recurrence, Successful Respondent shall, as soon as possible, remove and replace such Successful Respondent Personnel with an individual of suitable ability and qualifications, at no additional cost to DIR. Nothing in this provision shall operate or be construed to limit Successful Respondent's responsibility for the acts or omissions of Successful Respondent Personnel or be construed as joint employment of the Successful Respondent Personnel.

#### 5.4.4. Successful Respondent Personnel

- (a) The Successful Respondent is required to maintain CJIS compliance with staffing. Prior to the date any Successful Respondent personnel are assigned to DIR's or any DCS Customer's account, and annually thereafter, background checks (including national fingerprint record checks and drug testing) and/or criminal history investigations of such Successful Respondent personnel specified in the Service Management Manual or the applicable Statement of Work must be performed. Should any Successful Respondent personnel not meet CJIS compliance as a result of a background check and/or criminal history investigation, then Successful Respondent shall promptly replace the individual(s) in question. Successful Respondent personnel who do not meet CJIS compliance shall not be assigned to work hereunder.
- (b) Successful Respondent shall be responsible for verifying:
  - (i) that Successful Respondent personnel are authorized to work in any location in which they are assigned to perform Services,
  - (ii) that it has performed pre-hire background investigations, including those described within this Agreement, and
  - (iii) that Successful Respondent personnel had not been convicted of or accepted responsibility for a felony criminal offense or a misdemeanor involving moral turpitude. If such conviction has occurred, Successful Respondent shall fully advise DIR of the facts and circumstances surrounding the convictions so that DIR may determine if such individual may be permitted to work under this Agreement.
- (c) Successful Respondent shall maintain policies prohibiting the use of illegal drugs. Successful Respondent represents that the Successful Respondent personnel are not disqualified from performing their assigned work under applicable Laws.
- (d) The Successful Respondent shall, at a minimum:
  - (i) Limit access to and use of data to authorized Successful Respondent personnel only.
  - (ii) 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, DCS Customer Facilities, Systems, Networks or Data.
    - A. 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. Results of the initial

background check and all annual reverifications must be documented in the MSI’s Security Clearance and Tracking System.

- B. Background and criminal history background checks will be performed by the Texas Department of Public Safety and the Texas Department of Criminal Justice. DCS Customers may require additional levels of compliance as per agency regulations and policies. Successful Respondent shall comply with any such additional levels of compliance including but not limited to CJIS.
  - C. Successful Respondent is responsible for any costs associated with the criminal history background check process.
  - D. 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.
- (iii) 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.

**5.5. Location of Services**

- (a) Services are to be performed at a combination of sites which must include the State of Texas computing locations. Permanent office space in the ADC and SDC is available for Successful Respondent Staff. There is no charge for the use of this space. Respondents must indicate in their Response whether it intends to make use of this space and for what number of staff. DIR prefers Successful Respondent staff to be located in ADC or SDC offices.
- (b) All services and data must remain within the United States. Offshore access to any element of the Solution, Service, State specific deliverables, work products, technical details, or other data is not permissible under any circumstances.

**5.6. Work Location(s) and Successful Respondent Personnel Involvement**

- (a) The Respondent shall provide a summary of FTE personnel needed for service delivery and space planning considerations that includes completion of the following table:
  - (i) The values in this sample table are for **illustration purposes only**, Respondents are to remove these illustrative artifacts and populate the table based on their proposed team and work locations. **Rows may be changed or added to by Respondents.**

**Table 5 FTE Personnel and Space Considerations**

Respondent Proposed Role(s)	% of FTE Time Spent at ADC	% of FTE Time Spent at SDC	% of FTE Time Spent at Successful Respondent Work Location	Engagement Period
<b>MANAGED SERVICES ROLES</b>				
Successful Respondent Account Representative	20%		20%	Contracted duration
Successful Respondent Account Representative	100%			Contracted duration
Operations Service Lead	100%			Contracted duration
Security Systems Lead	100%			Contracted duration

Respondent Proposed Role(s)	% of FTE Time Spent at ADC	% of FTE Time Spent at SDC	% of FTE Time Spent at Successful Respondent Work Location	Engagement Period
Operating Systems Lead	50%			Contracted duration
Storage / Backup Systems Lead	Periodic		100%	Contracted duration
Virtualization Engineer	Periodic, 10%		Periodic, 20%	Contracted duration
Cloud Technical Architect(s)	100%			Contracted duration
Cloud Solutions Architect(s)	Periodic		50%	Contracted duration
Cloud Portfolio Architect	Periodic		100%	Contracted duration
Performance and Capacity Engineer	10%		90%	Contracted duration

- (b) FTE time shall represent those hours in direct support of DCS Customer business. In some cases, this number may be less than 100%.
- (c) The Respondent’s Service Staffing Plan and Time Commitment response must contain the following information:
- (i) An organizational chart including any subcontractors and key management and administrative personnel assigned to this project; and
  - (ii) A contingency plan that shows the ability to add more staff if needed to ensure meeting DCS Customer requirements.
- (d) The Respondent also must include a statement indicating to what extent, if any, the candidates may work on other projects or assignments during the term of the Contract. DIR may reject any Proposal that commits the proposed Project Manager or any proposed Key Project Personnel to other projects during the term of the Project, if DIR believes that any such commitment may be detrimental to the Respondent’s performance.
- (e) All services and data, including the transport of data, must remain within the contiguous United States. Access to any element of the Solution, Service, State specific deliverables, work products, technical details or other data is not permissible outside the contiguous United States under any circumstances.

### 5.7. Evergreen Service Personnel

- (a) Based on DIR’s experience with similar managed services relationships with a variety of leading vendors, DIR will regularly review that the Successful Respondent team (as a team and as individuals) regarding several key factors including, but not limited to:
- (i) Enablement of DIR Service-related initiatives.
  - (ii) Attainment of high customer satisfaction in Stakeholder DCS Customer communities and by extension and importantly end-user communities.
  - (iii) Creation of a highly integrated, collaborative, and mutually supportive delivery of Services under this Service to DCS Customers through the formation of an “integrated team” culture.
  - (iv) Adoption, implementation, and refinement of a “State First” operating culture that is designed to drive value through the relationship and result in a high-performance working partnership between DIR and Successful Respondent.
  - (v) Incorporation of industry-leading and Successful Respondent best practices in the operation, maintenance and support of the Service while seeking opportunities for continuous refinement

**State of Texas** Department of Information Resources, Data Center Services

and improvement of areas that are directly within the Successful Respondent's scope, those areas where the Successful Respondent has a reliance on DIR, the MSI, DCS Customers and third parties, and areas in the common interest of driving Service efficiency, quality and timeliness (e.g., value).

- (b) DIR and the Successful Respondent will meet on a regular basis, no less frequently than annually, to review the Successful Respondent's performance (as a team and as individuals) in driving toward these goals and agree to make changes to the number, nature, mix, or named Key Personnel as required to improve and enhance the Successful Respondent's position in enabling DIR's attainment of these goals. As a one-time evaluation, the Successful Respondent and DIR shall review the performance of the entire Successful Respondent team within ninety (90) days of the Effective Date of this Agreement as required herein and implement any changes such that the Service is launched with the best possible Successful Respondent team as possible.
- (c) Should, for whatever reason, DIR determine based on documented or observed performance that a member (or members) of the Successful Respondent's Key Personnel is operating in a manner inconsistent with these goals, DIR will request a meeting of the Successful Respondent Account Representative and the DCS Administrator (and, if required, the State CIO, Successful Respondent Managing Director, Lead Partner for Public Sector or equivalent) to address localized or endemic failures to meet these goals. Upon receiving this feedback, the Successful Respondent will develop and implement a plan to either realign the performance of the Key Personnel in question or replace them promptly should the situation dictate in accordance with the provisions of this RFO pertaining to replacement personnel.
- (d) For the avoidance of doubt, should for whatever reason the DCS Administrator request the replacement of any member of the Successful Respondent Staff, the Successful Respondent shall implement the change on a mutually agreeable schedule.
- (e) Should, for any reason described above DIR and Successful Respondent determine that a member of the Successful Respondent Key Personnel need replacement, this replacement shall occur no later than thirty (30) calendar days from DIR's request or as agreed.

### **5.8. Key Service Personnel**

- (a) In addition, the Respondent's proposal must identify all Key Service Personnel who will provide services as part of the resulting Contract. The Key Service Personnel are identified in Section 6.2 of this Exhibit. DIR expects the proposed named Key Service Personnel will be available as proposed. Resumes for the proposed candidates must be provided for all Key Service Personnel. Representative resumes are not acceptable. The resumes will be used to supplement the descriptive narrative provided by the Respondent regarding their proposed team.
- (b) The resume (two (2) page limit per resume) of the proposed Key Service Personnel must include:
  - (i) Proposed Candidate's Name;
  - (ii) Proposed role on this Service;
  - (iii) Listings of competed projects (a minimum of two (2) references for each named Key Project Personnel) that are comparable to this Project or required similar skills based on the person's assigned

**State of Texas** Department of Information Resources, Data Center Services

role/responsibility on this Project. Each project listed should include: at a minimum, the beginning and ending dates, client/company name for which the work was performed, client contact information for sponsoring Directors, Managers or equivalent level position (name, phone number, email address, company name, etc.), project title, project description, and a detailed description of the person's role/responsibility on the project;

- (iv) Education;
- (v) Professional Licenses/Certifications/Memberships; and
- (vi) Employment History.

(c) Based on DIR's experience with similar managed services relationships with a variety of leading vendors, DIR feels strongly that the Successful Respondent team (as a team and as individuals) should be regularly reviewed regarding several key factors including, but not limited to:

- (i) Enablement of DIR Service-related initiatives;
- (ii) Attainment of high customer satisfaction in Stakeholder DCS Customer communities and by extension and importantly end-user communities;
- (iii) Creation of a highly integrated, collaborative, and mutually supportive delivery of Services under this Service to DCS Customers through the formation of an "integrated team" culture;
- (iv) Adoption, implementation, and refinement of a "State First" operating culture that is designed to drive value through the relationship and result in a high-performance working partnership between DIR and Successful Respondent; and
- (v) Incorporation of industry-leading and Successful Respondent best practices in the operation, maintenance, and support of the Service while seeking opportunities for continuous refinement and improvement of areas that are directly within the Successful Respondent's scope, those areas where the Successful Respondent has a reliance on DIR, the MSI, DCS Customers and third parties, and areas in the common interest of driving Service efficiency, quality and timeliness (e.g., value).

(d) DIR and the Successful Respondent will meet on a regular basis, no less frequently than annually, to review the Successful Respondent's performance (as a team and as individuals) in driving toward these goals and agree to make changes to the number, nature, mix or named Key Personnel as required to improve and enhance the Successful Respondent's position in enabling DIR's attainment of these goals. As a one-time evaluation, the Successful Respondent and DIR shall review the performance of the entire Successful Respondent team within ninety (90) days of the Effective Date of this Contract as required herein and implement any changes such that the Service is launched with the best possible Successful Respondent team as possible.

(e) Should, for whatever reason, DIR determine based on documented or observed performance that a member (or members) of the Successful Respondent's Key Personnel is operating in a manner inconsistent with these goals, DIR will request a meeting of the Successful Respondent Account Representative and the DCS Administrator (and, if required, the State CIO, Successful Respondent Managing Director, Lead Partner for Public Sector or equivalent) to address localized or endemic failures to meet these goals. Upon receiving this feedback, the Successful Respondent will develop and implement a plan to either realign the performance of the Key Personnel in question or replace them promptly should the situation dictate in accordance with the provisions of this RFO pertaining to replacement personnel.

- (f) For the avoidance of doubt, should for whatever reason the DCS Administrator request the replacement of any member of the Successful Respondent Staff, the Successful Respondent shall implement the change on a mutually agreeable schedule.
- (g) Should, for any reason described above DIR and Successful Respondent determine that a member of the Successful Respondent Key Personnel need replacement, this replacement shall occur no later than thirty (30) calendar days from DIR's request or as agreed.

### **5.9. Personnel Experience, Accreditation and Certification Requirements**

The Successful Respondent shall be responsible for securing and maintaining staff that meets the minimum education qualifications as described in the Exhibit and possess the stated experience and expertise required to complete the tasks outlined in this RFO.

### **5.10. Transition Staffing Requirements**

The Successful Respondent must ensure an effective and successful transition of Services that ensures the Successful Respondent operations staff are sufficiently trained and prepared to assume operations. The Successful Respondent should ensure that Transition staff are not required to perform transition work post Commencement. Knowledge transfer must be performed such that steady-state operations personnel are prepared to perform Services with minimal to no disruption in performance.

## **6. Performance Model and Service Level Agreements**

- (a) As of the Commencement Date (or as otherwise specified), the Successful Respondent will meet or exceed all applicable Service Levels monthly, or as otherwise specified in the specific Service Level. Any Service Level Defaults prior to the Service Level Credit Start Date will not be considered in the evaluation of a Service Delivery Failure.
- (b) Key Performance Indicators, Critical Service Levels, Key Service Levels, Operating Measures, One Time Critical Deliverables and Recurring Critical Deliverables may be added or substituted by DIR during the Term. For example, such additions or substitutions may occur in conjunction with changes to the environment and the introduction of new Service, Equipment, Software, or means of Service delivery – provided, however, that where such change is a replacement or upgrade of existing technology, there shall be a presumption of equivalent or improved performance.

### **6.1. General**

#### **6.1.1. General Performance Standards**

In addition to the Service Levels contained herein and in **Attachment 1.2 Service Level Matrix**, beginning on the Commencement Date, Successful Respondent shall perform the Services at levels of accuracy, quality, completeness, timeliness, responsiveness, and resource efficiency that are at least equal to those received by DIR **State of Texas** Department of Information Resources, Data Center Services

and the DCS Customers prior to such date. In addition, Successful Respondent shall perform the Services at levels of accuracy, quality, completeness, timeliness, responsiveness, resource efficiency, and productivity that are at least equal to accepted industry standards of first tier providers of services that are the same as or similar to the Services. The foregoing provisions of this Subsection shall not be deemed to supersede the Service Levels.

#### 6.1.2. Service Level Performance Standards

Beginning on the Commencement Date, Successful Respondent shall perform the Services so as to meet or exceed the Service Levels set forth in or otherwise in accordance with the Agreement.

#### 6.1.3. Corrective Action Plan

In the event that either (i) DIR reasonably determines that Successful Respondent has failed or is reasonably likely to fail to deliver the Services, or (ii) Successful Respondent has determined that it has failed or is reasonably likely to fail to deliver the Services, then DIR or Successful Respondent, as applicable, will notify the other Party of such failure (a "CAP Notice"). Concurrently with such CAP Notice, Successful Respondent will immediately take steps to mitigate any harmful effects of such failure, promptly (and in any event as soon as reasonably practical) perform a Root Cause Analysis, and prepare a corrective action plan (each a "**Corrective Action Plan**" or "**CAP**") with respect to such failure. If in DIR's judgment any such Correction Action Plan is not adequately addressing the failure, Successful Respondent will meet with DIR and its designees in accordance with Article **8** DCS Governance Model. Within thirty (30) calendar days of a CAP Notice, the Successful Respondent will provide DIR with a written plan (the "Corrective Action Plan") for improving the Successful Respondent's performance to address the failure identified in the CAP (CAP Failure Event), which shall include a specific implementation timetable and measurable success criteria. Within thirty (30) calendar days of plan submission, or such other timeframe agreed to by DIR, the Successful Respondent will implement the CAP, which will include making timely and appropriate investments in people, processes, and technology. In addition, the Successful Respondent will demonstrate to DIR's reasonable satisfaction that the changes implemented by it have been made in normal operational processes to sustain compliant performance results in the future.

#### 6.1.4. Additional Remedies

In the event that Successful Respondent fails to identify and resolve any problems that may impede or delay the timely delivery of the Services, without prejudice to DIR's other rights and remedies under the Agreement or at law or equity, Successful Respondent will immediately provide, at its sole cost and expense, all such additional resources as are necessary to identify and resolve any problems that may impede or delay the delivery of the Services. In addition, without prejudice to DIR's other rights and remedies under the Agreement or at law or equity, in the event of a CAP Failure Event, DIR may equitably reduce the Charges set forth in **Exhibit 2** in an amount reasonably estimated by DIR to account for the Services that DIR and/or the DCS Customers are not receiving or did not receive.

## 6.2. Service Level Credits

Successful Respondent recognizes that DIR is paying Successful Respondent to deliver the Services at specified Service Levels. If Successful Respondent fails to meet such Service Levels, then, in addition to other remedies available to DIR, Successful Respondent shall pay or credit to DIR the Service Level Credits specified in **Attachment 1.2 Service Level Matrix** in recognition of the diminished value of the Services resulting from Successful Respondent's failure to meet the agreed upon level of performance, and not as a penalty. Under no circumstances shall the imposition of Service Level Credits be construed as DIR's sole or exclusive remedy for any failure to meet the Service Levels Service Level Credits are not counted toward and are not subject to the overall cap on Successful Respondent's liability.

## 6.3. Shared and Related Service Levels and Types

- (a) To clarify how specific Service Levels are intended to be tracked and calculated, individual Service Levels may be generally categorized as one (1) of two (2) types, representing the way individual SCPs and the Successful Respondent are either individually or jointly responsible for the specific Service Level's performance. Service Level Credits assessed against each SCP (or Successful Respondent) will be calculated based on the specific SCP's (or Successful Respondent's) Service Level Invoice Amount, At-Risk Amount, and Allocation of Pool Percentage.
- (i) **Type R (related):** Type R Service Levels are related measures shared between the Successful Respondent and the MSI. Type R Service Levels for the Successful Respondent are measured in the aggregate, counting events for both the Successful Respondent and the MSI. For the SCP, the Type R Service Level measures a discrete subset of the same pool of events, the subset applicable to that SCP. The definition and descriptions of Type R Service Levels as well as the Service Level targets remain identical in the related agreements for both the Successful Respondent, the MSI and the applicable SCP(s) during the Term, unless otherwise documented as an exclusion in Service Level Definitions.
  - (ii) **Type U (unique):** Type U Service Levels are intended to measure Services that are specific to one (1) SCP's or the Successful Respondent's performance, and therefore are not shared.
- (b) The groupings described above are intended to clarify Service Level types for tracking purposes; none of the Successful Respondent's obligations as fully described in the Agreement are limited by these groupings.

## 6.4. Reporting

- (a) Unless otherwise specified, each Key Performance Indicator, Critical Service Level, Key Service Level, Operating Measure, Recurring Critical Deliverable, and One-Time Critical Deliverable shall be measured and reported by Customer and by DIR Shared Technology Service (DCS, MAS, Texas.gov, MSS, etc.) monthly. The Successful Respondent shall provide data to the MSI enabling the MSI to calculate and report Service Level performance. The Successful Respondent shall comply with the MSI's tools, processes, data and reporting formats. The format, layout, and content of any reports shall be agreed between DIR and the Successful Respondent. The MSI will publish the Successful Respondent's monthly performance reports by the 20<sup>th</sup> calendar day of each month. Reporting on One-Time Critical Deliverables is only required until all One-Time Critical Deliverables are received and approved by DIR.

- (b) The Successful Respondent shall provide DIR with direct, unaltered access to review and audit all raw data collection related to Service Levels.
- (c) The Successful Respondent will create and maintain detailed procedure documentation of its Service Level Agreement (SLA) process used to collect SLA data. The process documentation must include quality assurance reviews and verification procedures. The data collection process must be automated to the extent possible, and any manual data collection steps must be clearly documented, verified and auditable. All methods, codes, and automated programs must be documented and provided to DIR for validation and approval. The Successful Respondent must ensure it tests and validates the accuracy and currency of the documentation and collection process on a quarterly basis.

#### 6.4.1.Reports

Successful Respondent shall provide the MSI and DIR with:

- (i) Data and reports pertaining to the performance of the Services and Successful Respondent's other obligations under this Agreement sufficient to permit the MSI and DIR to monitor and manage Successful Respondent's performance,
- (ii) those reports described in **Appendix A Reports** and the SMM in the form and format and at the frequencies provided therein,
- (iii) those reports required elsewhere under the terms of this Agreement,
- (iv) those generated by DIR and the DCS Customers prior to the Commencement Date, and
- (v) such additional reports as DIR may identify from time to time to be generated and delivered by Successful Respondent on an ad hoc or periodic basis (all such reports, the "Reports").

#### 6.4.2.Back-Up Documentation

As part of the Services, Successful Respondent shall provide the MSI and DIR with such documentation and other information available to Successful Respondent (including original source documentation and data in its native format or in an alternative industry-standard format as requested by DIR) as may be requested by DIR from time to time in order to verify the accuracy of the Reports provided by Successful Respondent. In addition, Successful Respondent shall provide DIR with all documentation and other information requested by DIR from time to time to verify that Successful Respondent's performance of the Services is in compliance with the Service Levels and this Agreement.

#### 6.4.3.Correction of Errors

Successful Respondent shall promptly correct any errors or inaccuracies in or with respect to the SLA performance data and reports as part of the Services and at no additional cost.

### 6.5. Service Level Default

- (a) A Service Level Default occurs when performance for a particular Critical Service Level fails to meet the applicable Minimum Service Level. Service Level Credits shall not apply to Key Service Levels.
- (b) In the event of a Service Level Default, the Successful Respondent shall provide DIR credits as defined below:

**State of Texas** Department of Information Resources, Data Center Services

(i) **NOTE: Attachment 1.2 Service Level Matrix** describes the information required to calculate a Service Level Credit.

(ii) For each Service Level Default, the Successful Respondent shall pay to DIR, a Service Level Credit that will be computed in accordance with the following formula:

(iii) **Service Level Credit = A x B x C**

(iv) **Where:**

**A** = The Allocation of the Pool Percentage specified for the Performance Category in which the Service Level Default occurred as shown in **Attachment 1.2 Service Level Matrix**.

**B** = The Service Level Credit Allocation Percentage for which the Service Level Default occurred as shown in **Attachment 1.2 Service Level Matrix**.

**C** = The At-Risk Amount

(c) For example, assume that the Successful Respondent fails to meet the Service Level for a Critical Service Level, the Successful Respondent's Service Level Invoice Amount for the month in which the Service Level Default occurred was \$100,000 and that the At-Risk Amount is fifteen percent (15%) of these charges.

(i) Additionally, assume that Allocation of Pool Percentage for the Performance Category of such Critical Service Level is fifty percent (50%) and that its Service Level Credit Allocation Percentage is forty percent (40%).

(ii) The Service Level Credit due to DIR for such Service Level Default would be computed as follows:

A = 50% (the Allocation of Pool Percentage) multiplied by

B = 40% (the Service Level Credit Allocation Percentage) multiplied by

C = \$15,000 (fifteen percent (15%) of \$100,000, the Successful Respondent's corresponding Service Level Invoice Amount)

= \$3,000 (the amount of the Service Level Credit)

(d) If more than one (1) Service Level Default has occurred in a single month, the sum of the corresponding Service Level Credits shall be credited to DIR.

(e) In no event shall the amount of Service Level Credits credited to DIR with respect to all Service Level Defaults occurring in a single month exceed, in total, the At-Risk Amount.

(f) The total amount of obligated Service Level Credits shall be credited on the following month (i.e., defaults occurring in August shall be included in the September invoice).

(g) The Successful Respondent acknowledges and agrees that the Service Level Credits shall not be deemed or construed to be liquidated damages or a sole and exclusive remedy or in derogation of any other rights and remedies DIR has hereunder or under the Agreement.

## 6.6. Earnback

The Successful Respondent shall have Earnback opportunities with respect to Service Level Credits as follows:

(i) The Successful Respondent shall earn back fifty percent (50%) of a Service Level Credit for a given Service Level Default when Service Level Performance for the Service Level that experienced a default, meets or exceeds the Service Level Target for each of the three (3) Measurement Windows immediately following the Measurement Window in which the Service Level Default occurred. The remaining fifty percent (50%) may be earned back when Service Level Performance meets or exceed the Service Level

- Target for each of the three (3) Measurement Windows following the initial three (3) Measurement Windows and Earnback.
- (ii) Whenever the Successful Respondent is entitled to an Earnback, the Successful Respondent shall include such Earnback as a charge to DIR (indicated as an Earnback) on the same invoice that contains charges for the Measurement Window giving rise to such Earnback and include such information in the Successful Respondent's monthly performance reports.
  - (iii) Upon termination or expiration of the Agreement, Service Level Credits issued by the Successful Respondent are no longer subject to Earnback.

## 6.7. Additions, Modification, and Deletions of Service Levels

- (a) By written notice, DIR may add, modify, or delete Key Performance Indicators, Critical Service Levels, Key Service Levels, and Operating Measures as described below.
- (b) DIR will provide at least ninety (90) calendar days' notice that additions or deletions to Performance Measures, (which include the movement of Critical Service Levels to Key Service Levels and Key Service Levels to Critical Service Levels), or modifications to Service Level Credit Allocation Percentages for any Critical Service Levels, modifications to Critical Service Levels and Key Service Levels measurement methodologies, or additions or deletions to Recurring Critical Deliverables are to be effective. DIR may send only one (1) such notice (which notice may contain multiple changes) each calendar quarter. Movement of Critical Service Levels to Key Service Levels and Key Service Levels to Critical Service Levels does not constitute creation of new Service Levels.

### 6.7.1. Additions

DIR may add Service Levels in accordance with Section 7.7 Additions, Modification, and Deletions of Service Levels. Service Level commitments associated with added Service Levels will be determined as follows:

- (i) The Parties shall attempt in good faith to agree on a Service Level commitment using industry standard measures or third-party advisory services (e.g., Gartner Group, Forrester, etc.).
- (ii) With respect to this individual Service Level, the period between the Statement of Work (SOW) Commencement Date and the Service Level Effective Date shall be used as a validation period. The Successful Respondent and DIR will review the actual Service Level Performance during this validation period. If the Service Level Performance does not generally meet the Service Level Minimum, the Successful Respondent will create a corrective action plan subject to DIR's approval, and the Parties will extend the validation period (reset the Service Level Effective Date) by a mutually agreed period not to exceed three (3) months. The Successful Respondent will implement the corrective action plan and report on progress to DIR during the extended validation period. This process may be repeated if mutually agreed by the Parties. If the Parties eventually agree that the Services must be changed (e.g., staffing or Restoration time targets) or the Service Level Minimum must be revised, the Parties will enact such agreed changes through the Change Control Procedures.

### 6.7.2. Modifications

- (a) DIR may add Service Levels in accordance with Section 6.7 Additions, Modification, and Deletions of Service Levels.

- (b) The Successful Respondent may propose modifications to Service Level measurement methodology for DIR approval. Service Level measurement methodology may be modified by updating **Attachment 1.3** Service Level Definitions.
- (c) For any Service Level commitments associated with modified service levels, the Parties shall attempt in good faith to agree on a modification to current Service Level commitments using industry standard measures or third-party advisory services. In the event the Parties cannot agree on proposed modifications, **MSA Section 12 Dispute Resolution** applies.

#### 6.7.3. Deletions

DIR may delete Critical Service Levels or Key Service Levels by sending written notice in accordance with Section [6.7 Additions, Modification, and Deletions of Service Levels](#).

#### 6.7.4. Impact of Additions and Deletions of Critical Service Levels on Service Level Credit Allocation Percentages

- (a) When adding or deleting a Critical Service Level, DIR shall modify the Service Level Credit Allocation Percentages for the Critical Service Levels such that the total Service Level Credit Allocation Percentages for all Critical Service Levels sums to less than or equal to Pool Percentage Available for Allocation.
- (b) If DIR adds a Critical Service Level but does not modify the Service Level Credit Allocation Percentages for the Critical Service Levels then, until DIR so modifies such Service Level Credit Allocation Percentages, the Service Level Credit Allocation Percentage for such added Critical Service Level shall be zero (0).

#### 6.7.5. Modifications of Service Level Credit Allocation Percentages for Critical Service Levels

DIR may modify the Service Level Credit Allocation Percentages for any Critical Service Levels by sending written notice in accordance with Section [6.7 Additions, Modification, and Deletions of Service Levels](#). DIR shall modify the Service Level Credit Allocation Percentages for two (2) or more of the Critical Service Levels such that the sum of the Service Level Credit Allocation Percentages for all Critical Service Levels is less than or equal to the Pool Percentage Available for Allocation.

### 6.8. Service Delivery Failure: Corrective Action Plan

- (a) If three (3) Service Level Defaults for the same Critical Service Level occur in any six (6) month period, then upon such third occurrence, this shall be deemed a "Service Delivery Failure." Within thirty (30) calendar days of a Service Delivery Failure, the Successful Respondent will provide DIR with a written plan (the "Service Delivery Corrective Action Plan (CAP)") for improving the Successful Respondent's performance to address the Service Delivery Failure, which shall include a specific implementation timetable and measurable success criteria. Within thirty (30) calendar days of plan submission, or such other timeframe agreed to by DIR, the Successful Respondent will implement the Service Delivery Corrective Action Plan (CAP), which will include making timely and appropriate investments in people, processes and technology. In addition, the Successful Respondent will demonstrate to DIR's reasonable satisfaction that the changes implemented by it have been made in normal operational processes to sustain compliant performance results in the future.

- (b) The Successful Respondent will be liable for a Service Level Credit in an amount equal to one percent (1 %) of the then-current Service Level Invoice Amount (the "CAP Failure Credit") upon the occurrence of:
  - (i) a Service Delivery Failure, or
  - (ii) if the Successful Respondent fails to implement the Service Delivery Corrective Action Plan in the specified timetable, or
  - (iii) if after the implementation of the Service Delivery Corrective Action Plan performance has not consistently improved.
- (c) The CAP Failure Credit will be applied to the monthly invoice until the Successful Respondent has demonstrated effective Service delivery, as evidenced by either:
  - (i) no reoccurrence of the Service Level Defaults which triggered the applicable Service Delivery Failure for a rolling three (3) months, or
  - (ii) in DIR's judgment, the Successful Respondent has remedied the failure which caused such Service Delivery Failure.
- (d) The CAP Failure Credit will not be subject to Earnback. The Successful Respondent acknowledges and agrees that the CAP Failure Credit shall not be deemed or construed to be liquidated damages or a sole and exclusive remedy or in derogation of any other rights and remedies DIR has hereunder or under the Agreement. For purposes of clarity, the CAP Failure Credit is separate from and therefore additive to any other Service Level Credits due in a given month, even if the Service Level Credits are for Service Level Defaults related to the Service Delivery Failure. In no event shall the sum of the CAP Failure Credit and any Service Level Credits credited to DIR with respect to all Service Level Defaults occurring in a single month exceed, in total, the At-Risk Amount.

## 6.9. Service Level Improvement Plans

- (a) If the Successful Respondent fails to meet any Minimum Service Level for a Critical Service Level for any one (1) or more DCS Customers, or for the enterprise as a whole, the Successful Respondent shall follow the MSI's performance management process to provide DIR and DCS Customers' with a written Service Level Improvement Plan (SLIP) per customer for improving the Successful Respondent's performance to satisfy the Service Level within thirty calendar (30) days of the failure to meet the Service Level. The objective of a Service Level Improvement Plan is to identify the root cause and formulate corrective actions to move performance to acceptable levels, implement those actions, and to correlate implemented corrective actions with Service Level results. All SLIPs must contain information about the root cause of the Service Level miss and corrective actions. All approved SLIP corrective actions shall be measured in the Corrective Action SLA results. The Successful Respondent will track its progress in implementing the improvement plan, and it will report to Governance the status of such plan. The MSI will initiate a SLIP via the standard Problem Management Process when a Service Level underperforms. The Successful Respondent shall comply with the SLIP.
- (b) DIR may also require overall Service Level Improvement Plans for Successful Respondent performance not directly related to an SLA that is impacting service delivery.
- (c) Customer SLIPs are not required when the Critical Service Level for the performance period has a low volume of instances where the results missed the minimum. A Customer SLIP will be initiated when the

difference between the numerator and the denominator is  $>$  Minimum Miss Threshold, or, SLA breach occurrences are  $>$  Minimum Miss Frequency within the Minimum Miss Frequency Timeframe. The Minimum Miss Threshold, Minimum Miss Frequency, and Minimum Miss Frequency Timeframe values are defined in the SMM for each Critical Service Level.

#### 6.10. Service Level Escalation Event

- (a) A Service Level Escalation Event occurs, if:
- (i) The Successful Respondent asserts that it has been unable to perform all or a portion of the Services measured by a Type R Service Level solely as a result of the failure by another SCP or the MSI with whom it shares such Type R Service Level to perform obligations specified in the Successful Respondent's agreement with DIR, including its SOWs and the SMM, and
  - (ii) The Successful Respondent has performed its own obligations as set forth in the Agreement, including the SOWs and SMM, which actions shall include:
    - A. immediately notifying DIR, SCP(s) and MSI that such failure may result in a Service Level Default;
    - B. providing the SCP or MSI with reasonable opportunity to correct such failure to perform and thereby avoid the SCP or MSI non-performance;
    - C. documenting that it has performed its obligations under the Agreement notwithstanding another SCPs or MSIs failure to perform; and
    - D. notifying DIR that a corrective action has commenced.
- (b) Upon the occurrence of a Service Level Escalation Event, the Successful Respondent may escalate the SCP or MSI failure through the appropriate governance structure for resolution in accordance with Article [8 DCS Governance Model](#).
- (c) If the applicable governance committee has determined that the Successful Respondent has satisfied each of the requirements and obligations set forth above, such resolution shall include excusing the Successful Respondent's performance related to such failure and may include other actions as reasonably determined by DIR including appropriate changes to the SMM.

#### 6.11. Service Level Definitions

Refer to **Attachment 1.2 Service Level Matrix** and **Attachment 1.3 Service Level Definitions and Performance Analytics** for detailed SLA definitions and measurement methodologies.

#### 6.12. Recurring Critical Deliverables

- (a) Certain of the Successful Respondent's obligations under the Agreement are periodic obligations to deliver key Recurring Critical Deliverables. Refer to **Attachment 1.1 Deliverables** and **Attachment 1.2 Service Levels Matrix** for amounts payable and frequency and. Imposition of a Recurring Critical Deliverables Credit for failure to meet the Recurring Critical Deliverables obligations shall not be subject to or included in the At-Risk Amount. The total amount of Recurring Critical Deliverables Credit that the Successful Respondent will be obligated to pay to DIR shall be reflected on the invoice that contains charges for the month following which the Recurring Critical Deliverables Credits accrued (for example, the amount of Recurring Critical Deliverables Credits payable for failure to deliver any Recurring

**State of Texas** Department of Information Resources, Data Center Services

Critical Deliverable(s) in August shall be set forth in the invoice for September charges issued in October). Under no circumstances shall the imposition of the Recurring Critical Deliverables Credit described above, or DIR's assertion of any other rights hereunder be construed as DIR's sole or exclusive remedy for any failures described hereunder.

- (b) DIR may add, modify, or delete Recurring Critical Deliverables by sending written notice, provided that after the implementation of any such addition or modification the aggregate amount of the Recurring Critical Deliverables Credits will not exceed the maximum amount of Recurring Critical Deliverables Credits set forth in **Attachment 1.2 Service Level Matrix**.

#### **6.13. One-Time Critical Deliverables – After Effective Date**

Certain of the Successful Respondent's obligations under the Agreement are one-time or periodic obligations to deliver One-Time Critical Deliverables. Refer to **Attachment 1.1 Deliverables** and **Attachment 1.2 Service Level Matrix** for amounts payable and frequency and. Imposition of Deliverable Credits for failure to meet the One-Time Critical Deliverables obligations shall not be subject to or included in the At-Risk Amount. The total amount of Deliverable Credits that the Successful Respondent will be obligated to pay to DIR shall be reflected on the invoice that contains charges for the month following which the Deliverable Credits accrued (for example, the amount of Deliverable Credits payable for failure to deliver any One-Time Critical Deliverable(s) in August shall be set forth in the invoice for September charges).

#### **6.14. Data Collection and Measuring Tools**

- (a) The Successful Respondent shall propose, and upon DIR's written approval, implement, a data collection methodology for all Service Levels prior to the date upon which the Successful Respondent shall be responsible for Service Level performance. Failure to do so may be deemed a Service Level Default for the Service Level until the Successful Respondent proposes and implements such acceptable data collection. All data collection tools must be integrated with the MSI's performance management and reporting tool.
- (b) Tools for new Service Levels will be implemented according to the Change Control Procedures. Upon DIR's written notice approving a proposed alternate or new measurement tool, such tool shall be deemed automatically incorporated into **Attachment 1.3 Service Level Definitions and Performance Analytics** as of the date for completion of implementation set forth in DIR's notification without requirement for an additional written amendment of this Agreement.
- (c) If, after the Effective Date or the implementation of tools for new Service Levels, the Successful Respondent desires to use a different data collection tool for a Service Level, the Successful Respondent shall provide written notice to DIR, in which event the Parties will reasonably adjust the measurements as necessary to account for any increased or decreased sensitivity in the new measuring tools; provided that, if the Parties cannot agree on the required adjustment, the Successful Respondent will continue to use the data collection tool that had been initially approved by DIR.

(d) It is not anticipated that changes in the data collection tools will drive changes in Service Levels; rather, the need to collect and accurately reflect the performance data should drive the development or change in performance monitoring tools. The Successful Respondent will configure all data collection tools to create an auditable record of each user access to the tool and any actions taken with respect to the data measured by or residing within the tool. All proposed tools must include functionality enabling such creation of an auditable record for all accesses to the tool.

**6.15. Percentage Objectives**

Certain Service Levels may not be measured against an objective of one hundred percent (100%); for example, time (days, hours, etc.), defects where zero (0) hours/days and zero percent (0%), respectively, are the appropriate objectives. The calculations described in this Section will be modified when appropriate to reflect these objectives.

**6.16. Low Volume**

(a) Some Service Levels are expressed in terms of achievement of a level of performance over a percentage of items occurring during a Measurement Window. In these instances, if the number of items occurring during a given Measurement Window is less than or equal to one hundred (100), the following algorithm will be used to determine the number of compliant items that Successful Respondent must successfully complete to achieve the Service Level concerned (Minimum Compliant Items), notwithstanding the percentage expressed in **Attachment 1.2 Service Level Matrix** as the target.

- (i) The number of items occurring during such Measurement Window shall be multiplied by the Service Level Target; and
- (ii) If the product of that multiplication is not a whole number, then such product shall be truncated to a whole number.

(b) For example, assume that a Service Level states that the Successful Respondent must complete ninety-five percent (95%) of incidents within four (4) hours to achieve this Service Level.

- (i) The following sample calculations illustrate how the above algorithm would function to determine the Minimum Compliant Items (incidents completed within four (4) hours) to achieve this Service Level, in each case given a different number of total incidents occurring during the corresponding Measurement Window:
- (ii) If the number of incidents is 100, the Minimum Compliant Items is 95 incidents (100 incidents x 95 percent = 95 incidents).
- (iii) If the number of incidents is 99, the Minimum Compliant Items is 94 incidents (99 incidents x 95 percent = 94.05 incidents, truncated to 94).
- (iv) If the number of incidents is nine (9), the Minimum Compliant Items is eight (8) incidents (9 incidents x 95 percent = 8.55 incidents, truncated to 8).

**Table 6 SLA Translation (Algorithm)**

Target	Service Level
Number of Items	Minimum Compliant Items
100	95
90	85
80	76
70	66

State of Texas Department of Information Resources, Data Center Services

Target	Service Level
Number of Items	Minimum Compliant Items
60	57
50	45
40	38
30	28
20	19
10	9

## 6.17. Service Level Review

### 6.17.1. Service Levels Review

- (a) **Initial Review:** Within six (6) months of the Service Commencement Date or completion of Transition as outlined in this Exhibit, whichever is sooner, or as agreed to by both parties, the Parties will meet to review the initial Service Levels and Successful Respondent’s performance and discuss possible modifications to the Service Levels. Any changes to the Service Levels will be only as agreed upon in writing by the Parties.
- (b) **Annual Review:** Every year following the Service Commencement Date or completion of Transition as outlined in this Exhibit, the Parties will meet to review the Service Levels and Successful Respondent’s performance in the period of time since the prior review and discuss possible modifications to the Service Levels. Any changes to the Service Levels will be managed according to the requirements in Section [6.7 Additions, Modification, and Deletions of Service Levels](#).

### 6.17.2. Temporary Escalation of a Key Service Level to a Critical Service Level

- (a) In general, Key Service Levels are considered measurable objectives by DIR and the SLA framework accommodates their treatment and importance to DIR. In the event that Successful Respondent performance is not meeting the established standards and requirements for Key Service Level related items, DIR may determine that a Key Service Level needs to be escalated to a Critical Service Level. The following conditions shall prevail in this escalation:
- (i) Successful Respondent performance falls below the Minimum Service Level for a Key Service Level for three (3) consecutive months; or
  - (ii) Successful Respondent performance is consistently below the Minimum Service Level for four (4) of any six (6) consecutive months.
- (b) Should one (1) or more of these conditions exist, DIR may:
- (i) Temporarily replace any Critical Service Level of its choosing with the Key Service Level until such time as the below standard SLA is determined to be consistently (i.e., more than three (3) months in a row) performing to standard; and
  - (ii) Promote the Key Service Level to the Critical Service Level modify the Service Level Allocation Percentages for the Critical Service Levels such that the total Service Level Credit Allocation Percentages for all Critical Service Levels sums to less than or equal to Pool Percentage Available, until such time as the below standard SLA is determined to be consistently (i.e., more than three (3) months in a row) performing to standard.

- (c) At the conclusion of three (3) consecutive months where the escalated Key Service Level is deemed to be performing at or above the Minimum Service Level, DIR may revert the escalated Key Service Level (now a Critical Service Level) back to its Key Service Level.

### 6.18. Key Performance Indicators

- (a) DIR requires Key Performance Indicators (KPIs) calculated on a dynamic, near real-time basis, utilizing the most current data. There will also be a need to report the KPIs on a monthly basis for governance purposes; however, the intent is to provide DIR with continuous updates throughout the month to facilitate strategy around future business direction. Weightings for the Operating Measurements (OM) will be maintained in the SMM.
- (b) The qualitative descriptions of the KPIs are set forth in **Attachment 1.3 Service Level Definitions and Performance Analytics**. The strategic objectives and commencement of obligations associated with such Key Performance Indicators are set forth in **Attachment 1.2 Service Level Matrix**. KPIs are not Service Levels and are not subject to Service Level Credits.
- (c) DIR's use of KPI's is for the sole purpose of accurately measuring the health of the Shared Services Program and while DIR retains the right to adjust numeric ratings at its sole discretion, DIR will collaborate with the Successful Respondent and SCPs to identify appropriate numeric ratings for the KPIs.

### 6.19. Operating Measurements

- (a) The qualitative descriptions of the OMs are set forth in **Attachment 1.3 Service Level Definitions and Performance Analytics**. These are linked to the KPIs as described in Section [6.18](#) and **Attachment 1.3 Service Level Definitions and Performance Analytics**. The business objectives and commencement of obligations associated with such Operating Measurements are set forth in **Attachment 1.2 Service Level Matrix**.
- (b) To ensure visibility of progress toward business and strategic objectives, the Successful Respondent will report Operating Measurements.
- (c) To ensure the integrated and seamless delivery of the Services, the Successful Respondent is required to report Operating Measurements that measure the dependencies with each SCP.

### 6.20. Operational Reports

The Successful Respondent's responsibilities include, at a minimum:

- (i) Providing all Reports currently being provided by the Incumbent Service Provider, including:
  - A. Those Reports listed in **Appendix A Reports**, including those reports contemplated in **Appendix A Reports**, but not in production;
  - B. According to the format, content, and frequency as noted in **Appendix A Reports**;
  - C. In compliance with report specifications identified in a formal report development process (e.g., requirements, development, test, acceptance, production ready) to be completed for each designated Report prior to the Commencement Date.

- (ii) Providing ad hoc reports as requested by DIR in compliance with processes outlined in the Service Management Manual.
  - A. Where practical provide the capability for DIR and DCS Customers to request Reports based on standard data provided via the Portal.
  - B. Provide capability for DIR or DCS Customer to generate ad hoc reports via the reporting tool.
- (iii) Delivering all Reports requested within other documents that are referenced as requirements in other Exhibits.
- (iv) Modifying the format, content, and frequency of any Report as requested by DIR during the Term, subject to Change Management procedures.
- (v) At a minimum, provide all Reports via the Portal through a real-time web-accessible reporting dashboard.
- (vi) Provide access statistics for Reports presented via the Portal at the request of DIR.
- (vii) Providing soft or hard copies of Reports as requested by DIR.

### 6.21. Single Incident/Multiple Defaults

If a single incident results in the failure of the Successful Respondent to meet more than one (1) Service Level, DIR shall have the right to select any one (1) of such multiple Service Level Defaults for which it will be entitled to receive a Service Level Credit and will respond to the Successful Respondent's reporting of the multiple Service Level Default and request for selection by notifying the Successful Respondent of the selection within five (5) DIR Business Days. DIR shall not be entitled to a Service Level Credit for each of such Service Level Defaults.

### 6.22. Exceptions

The Successful Respondent shall not be responsible for a failure to meet any Service Level solely to the extent that such failure is directly attributable to any circumstances that excuse the Successful Respondent's performance in accordance with **MSA Section 5.2 Savings Clause**.

### 6.23. Exclusions

Any incidents or requests opened prior to Commencement Date by DIR are excluded from SLA measurements and will be tracked separately. Additional exclusions are indicated in **Attachment 1.3 Service Level Definitions and Performance Analytics**.

## 7. Transformation Projects

### 7.1. Transformation Principles

- (a) DIR seeks, **via Respondent Response to this Section 7**, to include details relevant to the scope, design, cost, timing, sequencing of the projects contained throughout Section 7.3 Transformation Projects: Methodology.

- (b) In general, these transformation projects are designed to drive an overall better service environment for DCS Customers and protects the principles, where applicable, outlined in the sections below.

#### 7.1.1. Operating Model Improvement Principles

- (a) Utilize a modern orchestration environment that is capable of on-premise and pure cloud transparency and interoperability; and
- (b) Drive to a single source of interaction and truth for all DCS Customers including customer developers, architects, fiscal, security and operations functions under a unified tool and process model while removing service impediments and duplicative/obsolete elements in order to drive to a logically integrated operating environment with fewer tools and manual methods.

#### 7.1.2. Standardization and Consolidation Principles

- (a) Drive to a single set of DCS operating systems (e.g., Windows, 1-2 Linux and no long-term use of Unix) and fewer versions (N or N-1) to significantly simplify the patch management (O/S) and vulnerability profile (application/access levels) of the DCS environment as decided by DCS Governance and decision-making processes;
- (b) Work with security and operations teams to focus on the most pressing vulnerabilities in the environment with monitoring, patching and remediation tools as to include vulnerability scans, remediation and patching as a service to eliminate false red flags, and enable DIR security professionals to focus on policy, standards, repeatability and efficacy in the controls of the DCS environment; and
- (c) Drive higher levels of consolidation, virtualization and standardization and reduce the complexity of managing the monitoring, vulnerability, and patching processes as to minimize manual labor and risk management in the DCS environment.

#### 7.1.3. Customer Engagement and Agility Principles

- (a) Evolve DCS to a solution orientation and a driver of positive business outcomes as measured through the eyes of the DCS customer – driving to a “no wrong door” approach and functioning as a true solution provider (as opposed to a series of infrastructure providers) is essential;
- (b) Participate in TSS systems development or migration efforts of DCS Customers that are embarking on application development, consolidation or legacy modernization roadmaps with flexible configuration and deployment of DCS infrastructure to implement these projects;
- (c) Work with the DCS TSS provider to help Customers design and specify new systems that leverage standardized DCS infrastructure to drive quality projects and rapid adoption of DCS services;
- (d) Create an integrated, solution-oriented DCS Customer capability that streamlines onboarding, service request, and service management processes that is expedient, transparent, and simple; and
- (e) Streamline and simplify all elements of DCS that include overly manual and personal knowledge intensive processes and are information/intervention-intensive and replace them with customer self-service and customer experience enabling processes, tools, and platforms.

#### 7.1.4. Architecture Principles

- (a) Security must be positioned as one of the main benefits of DCS. DIR and its DCS Customers require a highly collaborative DCS environment that fosters rapid, “right first time” provisioning and Incident/Problem/Change processes across all service elements that remove real or perceived obstacles to cross-cloud networking (between private cloud and public cloud operators); and
- (b) DCS Customers are increasingly expecting true hybrid clouds—no walls between public clouds and on-premise systems contained in this Exhibit.

### 7.1.5. Service Management and Orchestration Principles

- (a) All DCS services, particularly those in this private cloud Service, must be designed and operated to provide a single view of the enterprise including production/non-production and private/public cloud - from a DCS Customer experience perspective - for operations and maintenance, and importantly from a risk management/security perspective;
- (b) The Successful Respondent must include capabilities to ensure that all software – whether production, development, operating or security – is current, licensed, patched and supported regardless of where it is deployed is a core cost and risk management tool.

### 7.1.6. Backup/Restore and Data Loss Prevention Principles

- (a) The next generation DCS environment should be designed so that customer CISOs understand and support its capabilities and have assurances that DIR assets (data, computing platforms, and networks) are protected to the greatest extent possible; and
- (b) Ensure all Customer data and applications are backed up and provide a Service capability that drives all DCS servers/storage – regardless of legacy, consolidated or public cloud under a single strategy with a verifiable outcome (preferably with a single toolset or target) regarding protection of State data maintained in DCS storage and database assets.

## 7.2. Organization and Relationships of Transformation Projects

- (a) DIR has identified some initial transformational project opportunities to be performed, at DIR’s option, over the duration of any agreement arising from this Exhibit. DIR may add additional transformation projects at any time.
- (b) The scope of these projects may require active participation by DCS Customers, DCS Governance functions, the MSI and other DCS SCPs as to affect the required outcomes. Respondents, as part of their proposal to this Exhibit, must include a complete solution inclusive of all solution execution elements (e.g., hardware, software, etc.), project timing, target implementation date, and sequencing as well as representative project plans. These plans must convey the sequencing, dependencies and involvement of DIR and DCS Customers, as well as other elements deemed required by the Respondent to drive successful outcomes and high-performance results within the DCS environment. Respondents may sequence or repackage these projects (into smaller initiatives or larger programs) as they see fit as to drive the highest value for DIR and DCS Customers and as to illustrate their capabilities in performing the work.

**Table 7 Transformation Project(s)**

Transformation Project	Impacts and Outcomes				
	Customer Engagement, Support & Business Agility	Service Order Management and I/P/C Automation	Environment Simplification, Rationalization and Standardization	Security and Risk Management	Operating Cost and Complexity Reduction
<b>Optional Project 1:</b> Business Analytics and Reporting (BAR) Platform Service Requirements	<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>

### 7.3. Transformation Projects: Methodology

DIR acknowledges that many Respondents may have their specific methodologies which may be employed in the performance and execution of such projects, but, as a general framework, DIR offers the following as to convey its requirements for phasing of projects that must be incorporated into any Respondent-specific methodologies in performing such projects. The Successful Respondent, in addition to Transformation Project-specific deliverables, and their own project execution methodologies will incorporate all DIR minimum project standards and deliverables as contained in Article 7 [Transformation Projects](#).

#### 7.3.1. Transformation Projects: Minimum Standards and Requirements

- (a) DIR must be notified of any emergency maintenance activities that must be performed on internal or external components. A mutually approved procedure must be established by DIR and Successful Respondent.
- (b) The Successful Respondent must comply with the MSI's project and change management processes and requirements and **must include written DIR approval for any change to any element that could adversely impact users of the service (public, State or otherwise) or render a DCS Customer system that utilizes the service unavailable to the system's user community (public, State or otherwise).**
- (c) All identified or future Public Cloud Transformation Projects or major project initiatives must adhere to the project management delivery requirements as contained in this Exhibit unless otherwise agreed in writing with DIR.

#### 7.3.2. Requirements Confirmation and Analysis Requirements

Any Transformation project requires the Successful Respondent to thoroughly document the business, functional, technical, operating and security requirements and recommend changes which will improve the DCS Customer's business processes and requirements. In general, due to their size and involvement requirements of DCS stakeholders, DCS Customers and potentially other DCS SCPs, these projects involve a level of documentation and rigor that lend themselves to a multi-phase type of approach.

#### 7.3.3. Project 1: Business Analytics and Reporting (BAR) Platform Service Requirements

- (a) **This project is an optional project. There is an expectation that Respondent provide a solution based on the instructions and assumptions described in the RFRO Instructions.**
- (b) In addition to the requirements in this section that are pertinent to all Public Cloud Services, there are additional service element specific requirements that are pertinent to the optional DCS Business Analytics and Reporting (BAR) Platform and associated Services as follows.

##### 7.3.3.1. General Platform Requirements

DIR seeks to enable future concurrent DCS Customer projects that may have a variety of differing project considerations including:

- (i) Use of a variety of analytical tools, whether they be commercial, open-source or proprietary to a data analytics firm performing the work – the platform(s) DIR requires should be operating system agnostic (e.g., Windows, Linux or variants);
- (ii) Accommodate very high processor core configurations, memory models and high-performance storage pools that are capable of ingesting, indexing and assembling very large data sets that may include correlated and non-correlated attributes;
- (iii) Ease of provisioning, use, and decommissioning after an analytics project with scalability to allow for preliminary project setup through scalability to process the volumes of data required by any project; and
- (iv) Offering a tiered security model that accommodates DIR’s needs in consideration of the datasets in question including commodity hosting for public access to “open” data sets; private data access for Projects being performed on anonymized data; and hardened security for State data of a sensitive nature that cannot under any circumstances be exposed.

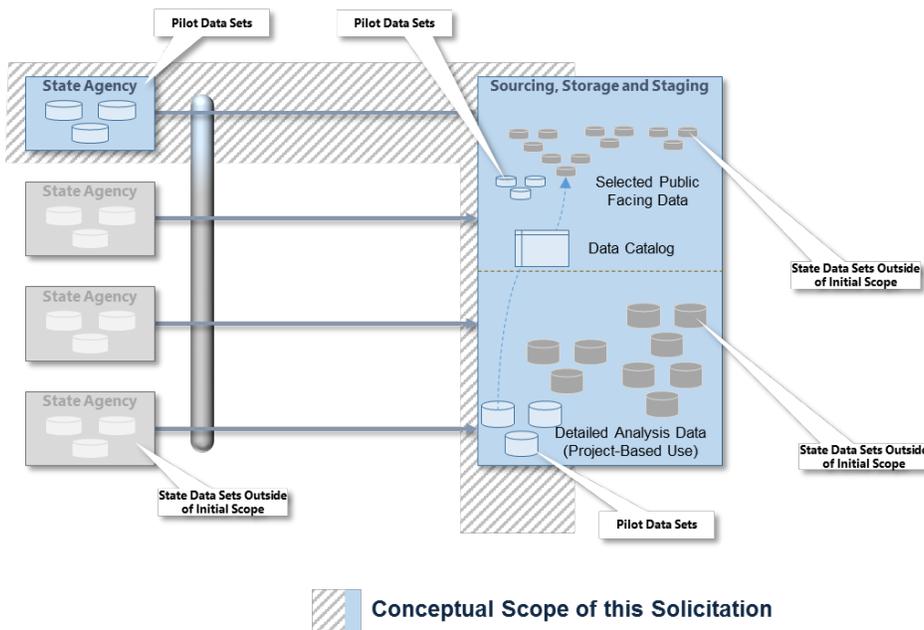
7.3.3.2. Conceptual Organization of Requirements and Scope of this Exhibit

(a) DIR has organized this Section in the following general categories. Specific requirements are contained later in this Section.

- (i) BAR Platform Technical Specification: Design and Implementation Services: including DIR requirements for the design and implementation of a multi-level (i.e., public, private, and protected) BAR capability for Customer analytics projects.
- (ii) BAR Application Management Services: operation, maintenance, application support of DCS Customer-developed Enterprise BAR applications.
- (iii) Optional Project Services: enhancements, projects and initiatives that leverage DIR’s Enterprise BAR platform for Enterprise or Customer benefit.

(b) Conceptually, the general scope of this Service is as follows:

7.3.3.3. General Project Conceptual Scope



7.3.3.4. Respondent Differentiators

Respondents should provide brief overviews of their capabilities, core competencies, and market differentiators in the following areas:

- (i) BAR technology platform specification, implementation, and operational services;
- (ii) Analytics/Reporting environment installation services including installation of data governance software as provided by the underlying BAR hardware platform(s); creation of a Hadoop-based processing environment; implementation of secure raw data storage for DCS Customer data set(s); and implementation of virtual/edge nodes for DCS Customer use in performing analytics and reporting projects;
- (iii) Related BAR application configuration, deployment and management services that may include reporting databases, performance tuning and management, operational/ongoing cost reduction projects, end-user rollout/training and other BAR-related activities; and
- (iv) Additional BAR advisory, support and implementation services that may be required to enable DCS Customer analytics and business reporting projects.

**7.3.3.5. Enterprise BAR Technical Specification, Design and Implementation Services**

- (a) DCS provides a private cloud that is offered to all State Agencies as an Enterprise Infrastructure as a Service (IaaS) platform for use in enabling the development, enhancements, and ongoing operations and maintenance of DCS Customer systems and applications. In general, this private cloud includes a variety of operating systems, predominantly supported versions of Microsoft Windows and prominent Linux distributions as well as elements of the cloud that utilize Unix. DIR has no preference for or bias against any of these operating systems and, provided supportability and compatibility considerations are met in enabling the technical elements of the BAR as well as commonly available operating systems/Linux distributions that are available in leading Public Cloud computing platforms that enable data analysis and reporting tools.
- (b) As part of their Response, Respondents should propose and, if awarded the work, as Successful Respondent design, implement, and deploy the following functional, technical and business elements that comprise the BAR platform.

**7.3.3.6. Enterprise BAR Solution Software and Components**

- (a) The Respondent shall identify, propose, design and implement a complete Enterprise BAR solution that meets or exceeds requirements contained in this Exhibit. Additionally, the Successful Respondent will adhere to DCS architecture, security and privacy requirements and include a complete set of tools and infrastructure the Successful Respondent believes DIR needs to provide the Enterprise BAR to DCS Customers as a Service to enable Customer-specific projects at a future date.
- (b) As part of its Response, the Respondent is to supply a complete listing of all components of the solution in a table to include the following information at a minimum (**NOTE**: cost information should be included in a similar table in the Respondent’s Cost Response Workbook).

**Table 7 Complete Listing of all Components of the Proposed Solution**

Software Name, Manufacturer, and Version	Component Name & Version Number	Commercial / Open Source	Basis of License / Unit of Measure (e.g., User, Cores, Enterprise, Unlimited)	Initial Sizing	Rationale for Selection and Summary of Functionality
Example (Delete)					

Software Name, Manufacturer, and Version	Component Name & Version Number	Commercial / Open Source	Basis of License / Unit of Measure (e.g., User, Cores, Enterprise, Unlimited)	Initial Sizing	Rationale for Selection and Summary of Functionality
Acme Corp: Widgetmaster for RedHat	UltraHadoop	Open Source	User	10	Hadoop Platform (Example)
Hadoop Platform Components (Production Operations)					
					[insert rows as required]
Hadoop Developer Components (Customer Projects – Assume Pilot Sizing)					
					[insert rows as required]
BAR to DCS Infrastructure Integration Tools / Elements					
					[insert rows as required]
BAR Ingestion and Loading Tools					
					[insert rows as required]
BAR Anonymization or Data Masking Tools					
					[insert rows as required]
Respondent Recommended / Optional Tools					
					[insert rows as required]

### 7.3.3.7. BAR Software Requirements

- (a) DIR requires solutions that comprise commercially supported Hadoop distribution that is included as a Leader in the Forrester Wave Big Data Hadoop Distributions, Q1 2016. The Hadoop distribution may be combined with other commercially supported open source, tools or commercial tools to provide a complete solution.
- (b) The total solution must be comprised of components that can be upgraded and maintained as new versions are available without custom integration or other custom coding being required to maintain the integrity of the solution. Software must be available to be installed in the Public Cloud and highly compatible with leading private cloud offerings available in the marketplace as to provide DIR the ability to interchangeably (or simultaneously) utilize DIR and Texas Private Cloud offerings for DCS Customer projects.
- (c) All server components must be installed, operated, and supported on the same operating system (OS) distribution and versions through all elements of the architecture on a consistent release, version and patch level at all times.

### 7.3.3.8. BAR Supported Data Types and Sources

- (a) The proposed and implemented BAR solution must support all data types supported by the Hadoop distribution which includes, but is not limited to, streaming, structured, and unstructured data types. Respondents may propose additional tools added to the BAR solution to extend the sources and types of data supported by the Hadoop distribution, but may not limit it in any way.
- (b) Data sources must, at a minimum, include structured and unstructured databases such as, but not limited to: MySQL, Oracle, Teradata, MSSQL Server, DB2, and other Hadoop solutions.
- (c) The Respondent will list all supported data sources, connectors, and data types that are included as proposed and available to DIR as options should DIR's need arise.

#### 7.3.3.9. BAR Compute, Processing, and Analytics

The Successful Respondent shall provide details pertinent to:

- (i) The proposed BAR solution's compute, processing, and analytics capabilities within the context of the DCS Customer-identified pilots as well as summary use cases and context and technical diagrams as needed. Responses must include details of the components and their respective capabilities and inherent limitations.
- (ii) Rationale for the inclusion of or any additional capabilities provided by the additional tools included in the BAR solution not part of the Hadoop distribution as part of the BAR or as an option for future consideration and DCS Customer use as appropriate.

#### 7.3.3.10. BAR Storage

The Successful Respondent shall provide details pertinent to:

- (i) The proposed BAR solution's storage capabilities with summary use cases and diagrams as needed.
- (ii) Pertinent details of the components and their respective capabilities and limitations and highlight any additional capabilities provided by the additional tools included in the BAR solution not part of the Hadoop distribution.

#### 7.3.3.11. BAR Ingestion and Integration

The Successful Respondent shall provide Data Ingestion and Integration Tools as to:

- (i) Maintain full fidelity data while enabling a full spectrum of data access from the raw full fidelity to the highly abstracted and de-identified access requirements.
- (ii) Provide version control to track, rollback and catalog ingested files as to ensure that all files are monitored, duplicate processing/loading does not occur, errant file(s) or data sources can be removed from the platform as well as the purging of obsolete or non-contemporary files or data sources should the DCS Customer require.

#### 7.3.3.12. BAR Data Sharing

- (a) The Respondent shall design and implement the proposed BAR solution's data sharing capabilities with summary use cases and diagrams as needed to meet the general sharing use cases (levels) outlined in this Section.

- (b) As part of their Response, Respondents must provide details and diagrams of the data sharing solution with focus on how DCS Governance, data management, and security requirements are addressed. Response must include details of the components and their respective capabilities and any limiting factors.
- (c) The Respondent shall design and implement methods to best organize data into multi-audience consumable information and publish data located across the State that is most important to Agencies, while strictly adhering to applicable State and Federal Laws and Customer policies. DIR has identified a three-level model for Respondents to provide as part of their Solution:
  - (i) Commodity / Public Access – those elements that are exposable (should the DIR require) to a general public audience that contains no private, personal, sensitive, financial or otherwise identifiable information;
  - (ii) State Private Access – those elements that may contain certain material, non-public information or otherwise not suitable for publication to the general public, but in general anonymized as to comply with applicable Federal and State laws and DCS Customer-specific requirements; and
  - (iii) State Protected Access – those elements that, while applicable to a DCS Customer’s needs, may contain source or raw data that has not been anonymized and/or by definition cannot be released or exposed under any circumstances outside selected personnel as determined by DIR.
- (d) Requirements for each of these levels are as follows:

**7.3.3.13. Commodity / Public Access Data Sharing Requirements**

- (a) DIR at some point in the future may elect to publish data as part of a “open data initiative” to better serve the public transparently (while protecting the privacy of our citizens and businesses) through a variety of methods including:

**Table 8 Open Data Initiative**

Example Users and Use	Representative Use Cases (Commodity / Public Access)
<b>Casual “Help me understand or find” Users</b>	<ul style="list-style-type: none"> <li>▪ Assisted web pages containing tabular, graphic or searchable data</li> <li>▪ Text or HTML documents</li> </ul>
<b>Proficient Users, Students and Interested Businesses</b>	<ul style="list-style-type: none"> <li>▪ Common Desktop Tool formats (DOCx, XLSx, HTML, XML)</li> </ul>
<b>Data Researchers, Scientists, Social, Environmental, Financial and Other Users</b>	<ul style="list-style-type: none"> <li>▪ Industry standard XML or CSV type machine readable formats that can be accessed and analyzed by common desktop software and most data/analytical tools</li> </ul>
<b>Data Professionals and Commercial Users internal and external to State government</b>	<ul style="list-style-type: none"> <li>▪ Industry standard XML or CSV type machine readable formats that can be accessed and analyzed by common desktop tools</li> <li>▪ JSON or RDF for high volume/highly volatile data sets that are intended to be combined with other data</li> </ul>

- (b) By definition, all data published or provided by DIR or DCS Customers at this level is devoid of any sensitive, proprietary, personally identifiable or otherwise identifying information. Respondents, as part of their response are to provide a BAR approach as part of their overall architecture to satisfy these requirements.

**7.3.3.14. State Protected Data Analytics Platform Requirements**

- (a) Some Customer Projects may contain data sets that are of a sensitive nature and protected under State and Federal laws (e.g., HIPAA, Family Educational Rights and Privacy Act (FERPA), IRS1075, etc.) which will be identified and disclosed to the Successful Respondent as part of any work. Should a condition occur where DIR or DCS Customers seek to leverage the BAR for such data, Respondents will incorporate in their proposal, and as Successful Respondents shall design and implement capabilities for DCS Customers to load and maintain such data.
- (b) **NOTE:** The Successful Respondent will not be exposed to live data that meets any of these criteria as part of this Project, but nonetheless will be required to deliver their solution in such a manner as to incorporate such data in the future.

#### 7.3.3.15. BAR Platform Governance and Security

- (a) The Successful Respondent shall design and implement a tool-aided data governance capabilities of the BAR solution as to:
  - (i) Monitor, enforce and verify the three (3) levels of data;
  - (ii) Driving validation activities that will be designed and implemented as part of the work;
  - (iii) Demonstrate best practices that will be implemented as part of solution; and
  - (iv) Include further details of the architectural components and their respective capabilities.
- (b) The Successful Respondent shall provide details and diagrams for the tool-aided security capabilities of the BAR solution that will be designed and implemented up as part of the work in support of the three-level model and the requirements for the platform.
- (c) Successful Respondents must include applicable best practices that will be implemented as part of the BAR solution.

#### 7.3.3.16. Implementation Project Deliverables and Milestones

As part of their response, Respondents should include details of their project design and testing capabilities with respect to the BAR solution.

#### 7.3.3.17. BAR Platform Management and Operations Requirements

The Successful Respondent shall design and implement tool aided data governance capabilities of the BAR solution to:

- (i) Operate and manage the end-to-end operation of the BAR inclusive of all data ingestion, storage, processing, and system functions that enable those capabilities; and
- (ii) Implement and utilize best practices part of the operations and maintenance of the solution include details of the components used for data and hub management and their respective capabilities.

#### 7.3.3.18. BAR Software and Environment Support Requirements

- (a) The Successful Respondent must install, configure, and test the complete BAR solution to support maintenance and patching, solution support, and production/non-production use as per the below table.

- (b) The Successful Respondent must provide monthly operations report for the BAR inclusive of:
  - (i) Routine Maintenance, Problem Management, Break/Fix Activities;
  - (ii) Completion of DIR-Scheduled Provisioning/De-Provisioning Activities;
  - (iii) System Uptime and Availability;
  - (iv) Provisioning and De-Provisioning of DCS Customer Project Administrative Users (e.g., root/dba);
  - (v) Job Scheduling and Performance of DCS Customer Data Ingestion/Anonymization Activities included within DCS Customer Projects; and
  - (vi) Environment Backup and Restoration Services.
- (c) Each installation must be fully documented and scripted/automated so that additional instances can be created in two (2) calendar days or less.
- (d) The solution instance must be able to grow horizontally to enable additional business requirements and performance. This horizontal growth must also be scripted/automated so that growth can be accommodated in less than eight (8) hours.
- (e) Respondent must specify and provide all software required to operate and maintain the BAR solution in its entirety inclusive of demonstration, DCS Customer development and production environments as follows:

**Table 9 BAR Solution Software**

Environment	Initial / Pilot	Customer Project Use / Production
Demo / Proof of Concept	1	3
Development	1	3
Quality Assurance/ Testing	1	3
Acceptance Testing	1	3
Production	1	3

- (f) This includes, but is not limited to:
  - (i) BAR software;
  - (ii) Infrastructure monitoring, analysis, and reporting; automated software provisioning and de-provisioning;
  - (iii) Automated and ad hoc backup using DIR provided virtual tape infrastructure, snapshot, clone, and recovery;
  - (iv) Utilization reporting by DCS Customer, program, or department of sizing, availability, performance, and utilization reporting;
  - (v) Hypervisor; container; server operating systems;
  - (vi) Networking; and service catalog and provisioning APIs;
  - (vii) Integrate with DCS Customer infrastructure monitoring, analysis, and reporting tools; firewall and networking between compute resources and storage (details of which are contained in this RFO); and
  - (viii) Integration to the MSI Portal for purposes of DCS Customer ordering and service management.

#### 7.3.3.19. DCS Customer Project Support Services

The Successful Respondent will participate in DCS Customer projects to:

- (i) Standardize the delivery model for DCS Customer use of the Enterprise BAR Solution;
- (ii) Facilitate smooth, well-defined transitions of new projects to steady-state/production support;
- (iii) Improve delivery through clearly defined development standards, conventions, and guiding principles;

- (iv) Implement a standards-based governance structure to drive process improvements and consistency across the platform;
- (v) Identify, design, and develop DCS Customer-specific security and data privacy requirements that follow State standards included in this RFO as well as any DCS Customer-specific requirements based on DCS Customer use of the Enterprise BAR platform.

#### 7.3.3.20. Changes Arising from Future Projects and Developments

- (a) From time to time, DIR may request that the Successful Respondent perform discrete services related to, or in connection with, the BAR Services. Any such DIR-requested project(s) will be further described and carried out pursuant to mutually agreed upon SOWs or applicable approved change orders.
- (b) Specific DIR or DCS Customer projects outside of the detailed Service, but that include the scope of Services required, may be arranged in one (1) or more mutually agreed upon SOWs.
- (c) Regardless of the origin of these services, the Successful Respondent must follow Contract change procedures. Based on the need to incorporate the ongoing operation, maintenance, and upgrades to these future projects over the term of the Contract, the Successful Respondent must enable any ongoing managed services requirements associated with the delivery of these projects to the applicable environment.

#### 7.3.3.21. Future Enterprise BAR Projects and Deployments: Successful Respondent Support Requirements

- (a) As a result of ongoing Enterprise BAR and application releases, stabilization and use by agencies, DIR has identified several opportunities for DCS Customers to leverage enterprise BAR solution-based projects that enable DIR's overall, and DCS Customer-specific, missions.
- (b) The Successful Respondent will engage in:
  - (i) The development and refinement of ongoing enterprise BAR business roadmaps for DIR-identified enterprise BAR opportunities;
  - (ii) The creation of business cases, change programs, enterprise BAR adoption/extension budgets, timelines and investment models that are pragmatic and grounded in the realities of budgets, implementation efforts and enterprise BAR capabilities;
  - (iii) Development and delivery of exploratory workshops with new DCS Customer groups from the above;
  - (iv) Leading of "change agent" type communications designed to encourage DCS Customer and Statewide adoption of enterprise BAR service offerings; and
  - (v) Participate in DCS governance in bridging: business, functional and technical and organizational changes to propose, design, implement and extend enterprise BAR offerings Statewide.

### 7.4. DCS Customer Managed Public Cloud Instances

- (a) The DCS Program has developed a strategy to optimize Public Cloud services and solutions for use by DCS Customers. There is a subset of DCS Customers who deployed environments in the Public Cloud (Legacy Managed), prior to the DCS program enablement of Public Cloud managed services and solutions. Currently, these environments are primarily DCS Customer managed. Due to the timing of these customer managed deployments, these environments were deployed outside the incumbent Public Cloud provider managed

service operating model, Reference Architecture and connectivity standards. It is DIR's intent for these environments to be assessed and transformed into DCS Managed services and solution standards.

- (b) There are 5 current DCS Customers who operate in a self-managed manner, with services being delivered in an inconsistent manner from Customer to Customer.
- (c) These 5 Customers will be referred to aligned to the defined Transformation projects identified below:
  - (i) Transformation Project 2
  - (ii) Transformation Project 3
  - (iii) Transformation Project 4
  - (iv) Transformation Project 5
  - (v) Transformation Project 6
  
- (d) The intent of this program is to bring all Public Cloud managed environments in alignment with the defined Cloud Service Tiers as defined in SOW Section 3.1.1. For purposes of this proposal, Respondent should assume the migrated end state for each Project to be aligned to the IaaS Semi-Managed Cloud Service Tier. Current volume detailed data feeds for Transformation Projects can be found posted to 436 Public Cloud Manager Data Room.
  
- (e) It is expected that solutions created to address the identified use cases will accelerate the time to value of DCS Customers to leverage a standard and scalable approach for enterprise support. Furthermore, the execution of the project should be completed in a manner reflective of the quality DCS Customers expect from their DCS services to further encourage the consumption of DCS Services that have been otherwise constrained by non-standard Public Cloud implementations.
  
- (f) Each of the Transformation Projects are consistent in that each DCS Customer has a level of self-management in the Public Cloud. What does vary and will be inconsistent from Customer to Customer may include:
  - (i) Access to environment
  - (ii) Monitoring and management tooling in use
  - (iii) Command Line Access requirements
  - (iv) Virtual Network design
  - (v) Backup requirements
  - (vi) IP Addressing
  - (vii) Public Cloud Services consumed
  
- (g) Given the dependencies on Security, potential Integration with Texas Private Cloud as well as application capabilities, it is expected the Successful Respondent will integrate with other SCPs (e.g., TSS, Texas Private Cloud, Network, Security) in the DCS program to achieve financially advantageous Customer solutions. To that end, Respondent should propose a solution that accomplishes:
  - (i) Identification and remediation of Customer environment gaps with DIR Reference Architecture standards

- (ii) Transfer the current Agency held agreement with the Public Cloud Provider to be moved under the DIR Agreement
- (iii) Align Customer environment to DIR standards:
  - A. Cloud connectivity
  - B. Networking standards
  - C. Virtual networking (e.g. VPC, VNET, IP Addressing, Subnetting, Routing tables, Network security groups, Firewalls, Regions/Availability zones)
  - D. Public Cloud services and support access standards
    - 1. SCP Support Model standards
    - 2. Cloud Security standards (including standard base level security and optional security services) as required to satisfy program Security policies
  - E. Monitoring and Administration
  - F. Disaster Recovery operations
- (iv) Enable standard security tools and processes
- (v) Enable standard operational support tools and processes aligned with program operational support models
- (vi) Enable customer consumption reporting and billing of public cloud compute services and correlated SCP support services consumed in alignment with standard MSI billing tools and process requirements
- (vii) Enable standard MSI operational tools, process, and program integration as required (i.e. incident, change, problem, event, CMDB, DR, SLA management)

#### 7.4.1. Project 2: Migration of DCS Customer Managed Public Cloud environment to Target State

- (a) Current Public Cloud Services Consumed
  - (i) AWS services consumed currently:
    - A. AmazonCloudWatch
    - B. AmazonDynamoDB
    - C. AmazonEC2
    - D. AmazonECR
    - E. AmazonECS
    - F. AmazonRDS
    - G. AmazonRoute53
    - H. AmazonS3
    - I. AmazonSNS
    - J. AmazonVPC
    - K. AWSCloudTrail
    - L. AWSCodeCommit
    - M. AWSDataTransfer
    - N. AWSDirectConnect
    - O. awskms
    - P. AWSLambda
    - Q. AWSQueueService
    - R. AWSSecretsManager
    - S. AWSSupportBusiness
    - T. CodeBuild

U. datapipeline

- (ii) Azure services consumed currently:
  - A. Microsoft.Compute
  - B. Microsoft.Network
  - C. Microsoft.RecoveryServices
  - D. Microsoft.Storage

(b) AWS OS Instance Count: 164

(c) Azure OS Instance Count: 67

#### 7.4.2. Project 3: Migration of DCS Customer Managed Public Cloud environment to Target State

(a) Current Public Cloud Services Consumed

- (i) AWS services consumed currently:
  - A. AmazonS3
  - B. AmazonSNS
  - C. AWSDataTransfer
  - D. awskms
  - E. AWSQueueService
  - F. AWSSecretsManager

- (ii) Azure services consumed currently:
  - A. Microsoft.Network

(b) AWS OS Instance Count: 37

#### 7.4.3. Project 4: Migration of DCS Customer Managed Public Cloud environment to Target State

(a) Current Public Cloud Services Consumed

- (i) AWS services consumed currently:
  - A. AmazonCloudFront
  - B. AmazonCloudWatch
  - C. AmazonEC2
  - D. AmazonGuardDuty
  - E. AmazonKinesis
  - F. AmazonKinesisFirehose
  - G. AmazonS3
  - H. AmazonSES
  - I. AmazonSNS

**State of Texas** Department of Information Resources, Data Center Services

- J. AmazonVPC
- K. AWSCloudTrail
- L. AWSDatabaseMigrationSvc
- M. AWSDataTransfer
- N. awskms
- O. AWSLambda
- P. AWSQueueService
- Q. AWSSecretsManager
- R. AWSSupportBusiness
- S. awswaf

(ii) Azure services consumed currently:

- A. n/a

(b) AWS OS Instance Count: 11

#### 7.4.4. Project 5: Migration of DCS Customer Managed Public Cloud environment to Target State

(a) Current Public Cloud Services Consumed

(i) AWS services consumed currently:

- A. AmazonCloudWatch
- B. AmazonDynamoDB
- C. AmazonEC2
- D. AmazonGuardDuty
- E. AmazonQuickSight
- F. AmazonRDS
- G. AmazonS3
- H. AmazonSNS
- I. AmazonVPC
- J. AmazonWorkDocs
- K. AmazonWorkSpaces
- L. AWSCloudTrail
- M. AWSConfig
- N. AWSDataTransfer
- O. AWSDirectConnect
- P. awskms
- Q. AWSLambda
- R. AWSQueueService
- S. AWSSecretsManager
- T. AWSSupportBusiness

(ii) Azure services consumed currently:

- A. Microsoft.ClassicCompute
- B. Microsoft.ClassicStorage
- C. Microsoft.Compute
- D. Microsoft.Network
- E. Microsoft.RecoveryServices
- F. Microsoft.Storage
- G. Virtual Network

- (b) AWS OS Instance Count: 86
- (c) Azure OS Instance Count: 89

#### 7.4.5. Project 6: Migration of DCS Customer Managed Public Cloud environment to Target State

##### (a) Current Public Cloud Services Consumed

###### (i) AWS services consumed currently:

- A. AmazonCloudWatch
- B. AmazonEC2
- C. AmazonGuardDuty
- D. AmazonRDS
- E. AmazonRoute53
- F. AmazonS3
- G. AmazonSES
- H. AmazonSNS
- I. AmazonVPC
- J. AmazonWorkDocs
- K. AmazonWorkSpaces
- L. AWSCloudTrail
- M. AWSDataTransfer
- N. AWSDirectConnect
- O. awskms
- P. AWSQueueService
- Q. AWSSecretsManager

###### (ii) Azure services consumed currently:

- A. n/a

- (b) AWS OS Instance Count: 11

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

- (a) During a ninety (90) day period immediately following the introduction of the Successful Respondent provided enhancements, configurations or extensions to the State's production environment the Successful Respondent must:
- (b) Ensure adequate staffing from the Successful Respondent Project Team is on hand (or available remotely) to ensure that during this 90-day period all defects identified by the State and mutually committed to resolve by the Successful Respondent in this Exhibit or under any SOW arising from this Exhibit are adhered to.
- (c) This responsibility shall specifically include:
  - (i) Prompt isolation, triage, and repair of any Severity 1 or 2 issues;
  - (ii) Performance Monitoring of the System to ensure that there are no statistically significant (i.e., plus five percent (+5%) deviations from actual production performance as compared to the system performance on a per-customer basis prior to the implementation of Successful Respondent developed elements;
  - (iii) All interfaces, and system functions perform and function as specified;
  - (iv) Compile all final versions of the upgrade documentation, work products and delivery materials and locate / organize them as 'FINAL' on the State provided SharePoint site; and
  - (v) Obtain a final acceptance document from the State and the Successful Respondent confirming that all of the above has been delivered and accepted as final.
- (d) If, during the ninety (90) day period immediately following the introduction to Production, a Severity 1 or 2 issue occurs that can be directly attributable to the efforts of the Successful Respondent, and not the State or other non-Project parties, the ninety (90) day period will, at the sole discretion of the State, be reset for additional ninety (90) day periods until such time as the system can perform for a full ninety (90) days without Severity 1 and 2 issues.

## 8. DCS Governance Model

### 8.1. Introduction

- (a) The Department of Information Resources (DIR) has established the owner-operator governance model for DIR's current shared technology services programs, which currently include:
  - (i) Data Center Services (DCS);
  - (ii) Managed Application Services (MAS);
  - (iii) Managed Security Services (MSS); and
  - (iv) Texas.gov.
- (b) This model involves DIR and DCS Customers at all levels in governance decision making, including as representatives on all governance committees. The owner-operator model focuses on resolving issues at the lowest possible level and driving for consensus-based solutions. Where consensus cannot be reached, processes include an escalation path. For greater detail on the owner-operator governance structure; the roles and responsibilities to maintain working relationships between the MSI and other SCPs, and the service management process, see the data room.

**State of Texas** Department of Information Resources, Data Center Services

- (c) The Successful Respondent will participate and work within the DCS Governance model as it relates to the requirements the Contract.

## 8.2. Governance: Meetings

### 8.2.1. Governance

The parties shall comply with the governance and account management provisions set forth herein.

### 8.2.2. Meetings

During the term of this Agreement, representatives of the Parties shall meet periodically or as requested by DIR to discuss matters arising under this Agreement, including any such meetings provided for in the Transition Plan and the Service Management Manual. During the Transition Period, this may include meetings with DIR, the incumbent vendor, and other DIR Service Component Providers. Each Party shall bear its own costs in connection with the attendance and participation of such Party's representatives in such meetings.

### 8.2.3. Member Responsibilities

DIR has invested in the owner-operator governance model as a best practice to promote proactive problem solving and effectively engage DIR, DCS Customers, and SCPs in a collaborative decision-making model. The Successful Respondent is responsible for meeting the requirements of an SCP as they relate to the governance model. The shared responsibilities for DIR, DCS Customers, and SCPs include:

- (i) Foster an environment of open and honest communications;
- (ii) Actively participate in governance processes, including providing input to issue discussions;
- (iii) Proactively enable communications distributed by DIR to enable effective issue resolution;
- (iv) Collaborate proactively to identify, report, document, and resolve at the lowest possible level:
  - A. Service delivery and performance issues;
  - B. Security services program issues;
  - C. Contract and financial issues;
  - D. Invoice disputes; and
  - E. Customer relationship and communications issues.
- (v) Document escalated issues with an appropriate level of detail to ensure resolution;
- (vi) Participate in the development of and compliance with governance process improvement; and
- (vii) Actively participate in training provided by DIR and others regarding the contract, services, performance, and stakeholder responsibilities.

### 8.2.4. Membership

DIR and DCS Customers are members of all solution groups and committees. SCP and MSI representatives are fully participating members of the solution groups and committees, except for the Contract and Finance Solution Group where they participate by invitation and do not participate in decision making. On the BELC, SCPs and the MSI participate in solutioning and consensus decision making, but in the rare event that the BELC cannot reach a decision by consensus, DIR and DCS Customer members may vote to reach a decision.

### 8.2.5.DCS Customer Member Responsibilities

Each DCS Customer partner group selects its representatives for all committees and solution groups. These members represent all the customers in that partner group. Members are expected to be prepared before attending meetings which includes:

- (i) Review all meeting materials in detail, especially partner agency comments, prior to committee meetings;
- (ii) Leverage technical resources from DIR or DCS Customer organization to build solutions;
- (iii) Facilitate effective communication and problem solving to promote resolutions;
- (iv) Communicate with partner groups as needed to prepare to represent their perspectives in discussions (DCS Customer committee members); and
- (v) Strive to effectively communicate positions of each DCS Customer (Customer committee members).

### 8.2.6.Partner Group Responsibilities

DCS Customers who are not on committees have responsibilities to support the process and communicate with their representative. These responsibilities include:

- (i) Resolve operational issues at the lowest possible level through local interfaces with SCPs;
- (ii) Actively participate in review of governance issues to be informed and serve as a substitute at a committee meeting if necessary;
- (iii) Engage and communicate with partner group representatives to support effective representation, issue resolution, and solution development; and
- (iv) Establish and maintain strong working relationships with partner group members.

### 8.2.7.DIR Responsibilities

DIR provides overall leadership and coordination for governance. In this role, DIR's additional responsibilities include:

- (i) Facilitate governance committee meetings and activities, including providing organizational, logistical, and communication support to all committees;
- (ii) Facilitate the issue management process, including developing an issue communication system giving all DCS Customers visibility into all issues;
- (iii) Triage issues and attempt immediate resolution if possible, and route unresolved enterprise issues to appropriate governance committees for resolution;
- (iv) Provide relationship management for customers including serving as a point of escalation for issue resolution;
- (v) Interpret the Agreement from DIR's perspective;
- (vi) Manage financial interactions, processes, and relationships with SCPs;
- (vii) Manage communications;
- (viii) Coordinate ongoing training related to Agreement changes, process changes, and New Services; and
- (ix) Perform vendor management and compliance functions including development and execution of Agreement amendments.

### 8.2.8.SCP and MSI Responsibilities

To enable the governance model, all SCPs have an important role as subject matter experts on technology, solutions, and feasibility. This includes the following responsibilities:

- (i) Engage directly with DCS Customers to resolve their specific operational issues at the local level;

- (ii) Assign empowered subject-matter experts to participate as requested in governance committees to resolve enterprise issues;
- (iii) Research, as necessary, and document SCP perspective for issue resolution papers;
- (iv) Provide timely and accurate data, information, and responses to promote prompt resolution of issues; and
- (v) Enable and facilitate use of the issue management process.

The MSI has additional governance responsibilities beyond those of the SCPs, including:

- (i) Providing DIR with the operational intelligence to select appropriate topics, issues, and opportunities for meeting agendas;
- (ii) Preparing agendas and presentation materials; taking meeting notes;
- (iii) Coordinating issue escalation when multiple SCPs are involved;
- (iv) Coordinating SCPs participation in governance meetings;
- (v) Offering process improvement solutions to reduce the number of escalated issues;
- (vi) Streamlining the issue escalation processes between SCPs;
- (vii) Coordinating implementation of decisions and solutions that are approved by the governance committees; and
- (viii) Posting all governance agendas, presentations, meeting notes, decisions, and policies on the Portal.

### 8.3. Issue Management

(a) Governance committees address two (2) types of decisions:

- (i) Issue resolution; and
- (ii) Strategic decisions as per the roles and responsibilities.

(b) Escalated issues may be raised from a DCS Customer, SCP, MSI, or DIR. DIR identifies and presents strategic decisions to governance committees and solution groups. Both decision types are treated the same by the committees:

- (i) All DCS Customers have an opportunity to hear the issue;
- (ii) DIR performs triage and routes unresolved issues to appropriate committees;
- (iii) All DCS Customers and all SCPs have an opportunity to provide their perspective to their partner group in advance of the meeting;
- (iv) DCS Customer committee members will review partner group positions/perspectives to represent their partner agencies in the meeting;
- (v) All SCPs can present their position to the committee or solution group;
- (vi) All decision-making agenda items will be broadcast in advance of the meeting; and
- (vii) After the meeting, decisions will be documented with the issue.

#### 8.3.1. Escalation Process

- (a) As noted above, the governance model strives to resolve issues at the operational level. However, not all issues will be resolved at this level, so the governance model includes an escalation process designed to route the issue promptly and efficiently to the appropriate committee for resolution. Most operational issues will be routed to a solution group; however, the ITLC is the first resolver for high profile business, technology, and financial issues.
- (b) After the DCS Customer and SCP determine an issue cannot be resolved at the local operational level, the issue is escalated to DIR. DIR triages and makes a further attempt to resolve. If resolution is not reached quickly, then DIR determines the appropriate committee for resolution and coordinates with the DCS Customer Committee chair or co-chair to determine when the issue can be placed on the agenda.

**State of Texas** Department of Information Resources, Data Center Services

- (c) DIR also coordinates with the DCS Customer and SCPs involved in the issue to complete the required documentation for DCS Customer input on the process as follows:
  - (i) DIR and the committee chair or co-chair coordinate the distribution of the issue material with the meeting agenda;
  - (ii) Meeting agendas and associated material are distributed to DCS Customer IT Directors in advance of the meeting, with approximately five (5) to seven (7) DIR Business Days for DCS Customers to review and provide input to their committee representative and approximately two (2) days for DIR to compile the comments received for distribution to all.

#### 8.3.2. Notice by Successful Respondent

Without limiting its obligations under this Agreement, Successful Respondent shall expeditiously notify DIR when it becomes aware that an act or omission of DIR or DCS Customer personnel or a DIR Contractor shall cause, or has caused, a problem or delay in providing the Services, and shall work with DIR, the DCS Customers and the DIR Contractor to prevent or circumvent such problem or delay. Successful Respondent shall cooperate with DIR, the DCS Customers and DIR Contractors to resolve differences and conflicts arising between the Services and other activities undertaken by DIR, the DCS Customers and DIR Contractors.

#### 8.3.3. Strategic Decision Process

- (a) Strategic program decisions may be required by the Agreement (e.g., Technology Plan) and, thus, follow a prescribed timing cycle or they may arise from a technical constraint, opportunity or business need. Regardless of the source, strategic decisions follow a similar process:
  - (i) DIR coordinates the development of background materials to explain the decision, implications for the enterprise, and any technical considerations that are relevant. This coordination may include the engagement of DCS Customer or SCP subject matter experts to create materials and complete technical analysis.
  - (ii) DIR develops a format for DCS Customer input appropriate for the decision.
- (b) DIR and the committee chair or co-chair coordinate the distribution of the issue material with the meeting agenda. Meeting agendas and associated material are distributed to DCS Customer IT Directors in advance of the meeting, with approximately five (5) to seven (7) DIR Business Days for DCS Customers to review and provide input to their committee representative and approximately two (2) days for DIR to compile the comments received for distribution to all.

#### 8.3.4. Decision Documentation

After the committee meeting, DIR documents decisions made and any follow up tasks such as updates to associated artifacts (e.g., SMM). Decisions are posted to the Portal for visibility by all Authorized Users.

## 9. Cross-Functional Services

### 9.1. General Operating Model Requirements

- (a) DIR contracts with multiple SCPs to deliver shared technology services to DCS 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.
- (b) DIR bases its Service Management practices on the Information Technology Infrastructure Library (ITIL). Accordingly, DIR requires that Successful Respondent Service Management practices, which are used to support the Services, be based on the ITIL framework and guidance as provided by the MSI.

### 9.2. Multi-sourcing Services Integration and Cooperation

Successful Respondent acknowledges and agrees that it will deliver the Services to DIR and DCS Customers in an environment in which there are various other Service Component Providers providing related services to DIR and DCS Customers ("Multi-sourcing Services Environment"). Successful Respondent acknowledges that its provision of the Services in a multi-supplier environment requires significant integration, cooperation, and coordination of processes and procedures with other Service Component Providers. **Attachments 1.2 Service Level Matrix and 1.3 Service Level Definitions and Performance Analytics** specify Service Levels and obligations to DIR and DCS Customers related to the provision of the Services in a multi-supplier environment.

### 9.3. Shared Technology Services Documentation – Service Management Manual

- (a) 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 this Section. All documentation must be posted and maintained on the MSI-managed DCS Portal.
- (b) The Successful Respondent shall, at a minimum:
  - (i) Ensure that Successful Respondent's operational procedures and documentation related to the Services is up to date, accurate, and posted on the MSI's Portal.
    - A. Link Systems documentation to architectural standards;
    - B. Identify DIR Data to the associated System(s) and the associated security risk classification; and
    - C. Provide architecture and design documentation for Systems and Services managed by Successful Respondent.
  - (ii) Develop and maintain Service support documentation on all Operations procedures, Services, Equipment, and Software for which Successful Respondent is responsible. Documentation shall be based on ITIL guidance to enable consistent management of process-driven IT services across a variable number of environments and among DCS SCPs.
  - (iii) Make all documentation available electronically on the MSI portal.
  - (iv) Validate documentation annually for completeness and accuracy in accordance with MSI SMM review cycle, and verify that all documentation is present, organized, readable, and updated in accordance with agreed upon schedule.

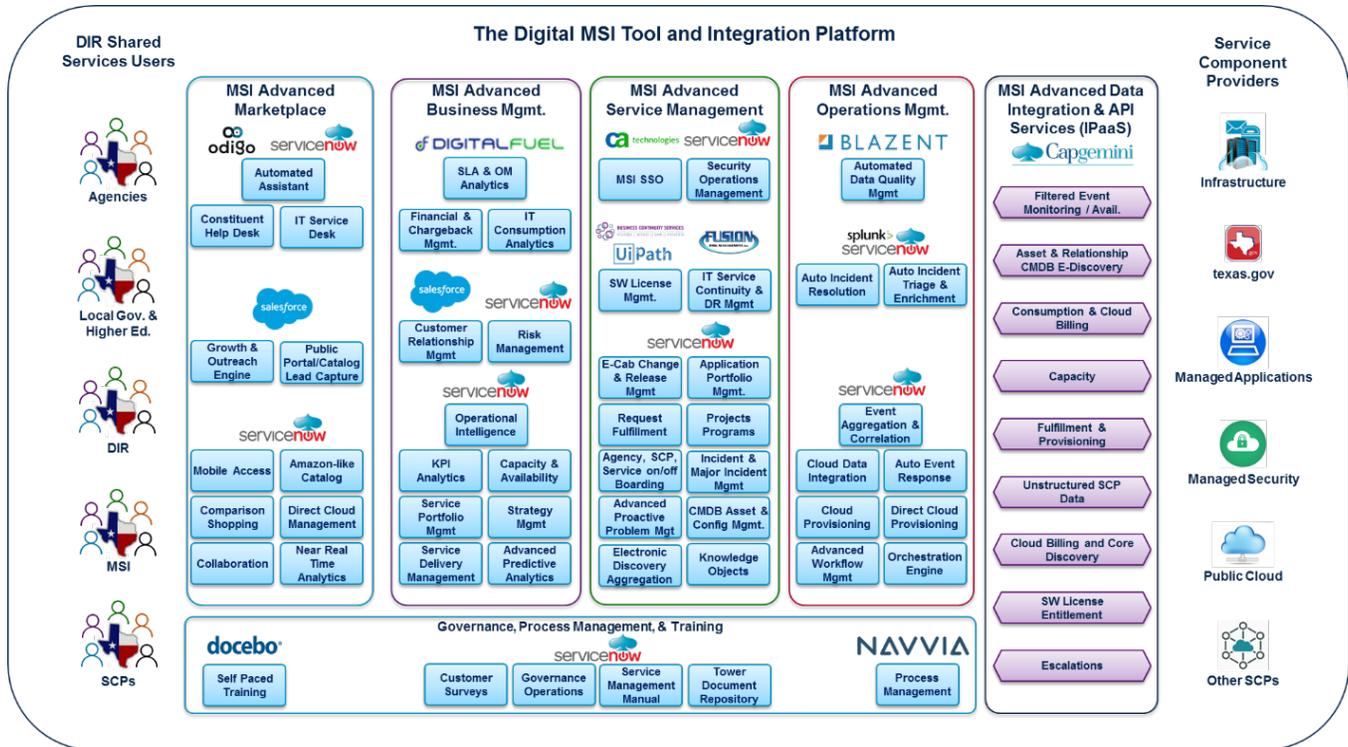
- (v) Participate in MSI review of operational documentation validation, including reporting any findings to DIR and DCS Customers on a scheduled basis. Where it is determined that documentation is inaccurate (e.g., erroneous or out of date), correct and replace such documentation.
- (vi) Update the SMM according to schedule described for the Critical Deliverables.
- (vii) Ensure that ITIL-based processes effectively integrate with the processes, functions and roles deployed within and used by DIR and DCS Customers and other DCS SCPs.
- (viii) Develop and support required Application Program Interfaces (APIs) to integrate and automate Service provisioning, automated build, and decommissioning activities.
- (ix) Design processes to enable the effective monitoring and reporting of the Services in a Multi-Supplier Environment.
- (x) Ensure that enterprise processes (e.g., Change Management, Configuration Management, Problem Management) are followed across the Service Component Provider and Third Party Vendor(s) processes.

#### 9.4. Marketplace and Portal Requirements

- (a) The Successful Respondent must leverage the MSI-provided Portal (Portal) to provide integrated DIR and DCS Customer solutions, communications, and reporting. Reporting functions and specific operational reports are defined in **Appendix A Reports**.
- (b) The Successful Respondent shall, at a minimum:
  - (i) Follow established MSI policies and procedures to ensure secure access to the MSI's DCS Portal, including identifying and working with MSI to resolve access issues;
  - (ii) Provide the MSI via direct data feed or system integration where possible with the reports and communication content to be posted, including but not limited to the following:
    - A. Processes;
    - B. Documentation;
    - C. Reports;
    - D. Operational intelligence;
    - E. Portal broadcast communications;
    - F. DIR Shared Services tool links; and
    - G. Information pertaining to the delivery of Services.
  - (iii) Develop and support Marketplace capabilities with API and automation to provide Customers with the ability to provision, modify, and decommission services and technology;
  - (iv) Provide reports and communication content in the format and design standards required of the MSI's online portal, and validate that content has been posted via MSI-provided secure access to the Portal;
  - (v) Leverage the Portal to access, update, and maintain DIR Shared Services documentation, including the following:
    - A. SMM;
    - B. Enterprise Policies;
    - C. Enterprise Standards and Reference Architectures;
    - D. Knowledge objects of Services;
    - E. Known errors and workarounds;
    - F. Training content;
    - G. Service Offering descriptions
    - H. Frequently Asked Questions (FAQs); and
    - I. Similar documentation for the Successful Respondent's organization as well as from other SCPs as specified by DIR; and
    - J. Adhere to established policies, procedures, and processes as documented in the SMM.

## 9.5. MSI Tools and Operating Environment

(a) The MSI provides a digital tool and integration platform for all DCS and Shared Services providers to utilize in the delivery of services to Customers. Conceptually, this platform is as follows:



(b) The foundation of this platform is the **ServiceNow** cloud-based platform which delivers on the requirements of DIR and the MSI and provides efficient scalability and flexibility to serve the State of Texas.

(c) Beyond ServiceNow, leading toolsets to fill in functions that are not currently resident in the ServiceNow platform to offer a complete operating environment that is based on ITIL and ITSM standards. This platform will continue to evolve in a plug and play fashion for the foreseeable future.

(d) The MSI toolset also includes:

- (i) **SalesForce.com** as the primary platform for the DIR Growth and Outreach function ;
- (ii) **Odigo** for the IT Service Desk and the new Citizen Help Desk Automation associated with Texas.gov and future “citizen centric” services;
- (iii) **Digital Fuel** for Financial Management, Chargeback, and SLA Reporting;
- (iv) **CA Technologies** for the Digital MSI SSO Identity and Access Management Services;
- (v) **BCS and UI Path** for Software License Compliance functions;
- (vi) **Blazent** for Data Quality Management;
- (vii) **Splunk** to capture un-structured data primarily from SCPs to aid in analysis and to use for Machine Learning data sets for identifying patterns that can be indicators of future incidents or outages;
- (viii) **MSI-specific IPaaS** which will serve as the integration platform as an enabler for deeper and faster API integration with SCPs;
- (ix) **Docebo** as the Learning Management Platform for the Digital MSI education functions;
- (x) **Fusion Risk Management** for Disaster Recovery enablement; and

**State of Texas** Department of Information Resources, Data Center Services

- (xi) Risk Management within the portal serves as a vital management approach for the overall Program, through identification and management of risk mitigation.

## 9.6. Service Catalog Management

The MSI provides the Service Catalog tool for DCS Customers to request Services from the Successful Respondent. The Successful Respondent shall, at a minimum:

- (i) Coordinate with the MSI to ensure automated integration of Successful Respondent Services into the Service Catalog, including integrating Successful Respondent fulfillment system with the Service Catalog (if applicable);
- (ii) Proactively recommend or request new Service Catalog items to increase customer self-service and satisfaction;
- (iii) Work with the MSI to categorize and normalize Service Catalog content, including the following:
  - A. Type of service;
  - B. Configuration type
  - C. Equipment or software type; and
  - D. User eligibility in order to enable multiple selection, searching, and presentation views;
- (iv) Work with the MSI to document and update Service descriptions and dependencies;
- (v) Participate, through the MSI, in regular communications with DIR and DCS Customers on updates to the Service Catalog; and
- (vi) Respond to Service Catalog requests in accordance with defined processes and Service Level Agreements (SLAs).
- (vii) Assist the MSI in Service Catalog evolution for Public Cloud services.

## 9.7. Outreach and Growth Requirements

- (a) Because DIR believes sustained growth and use of the Shared Technology Services will provide certain benefits to the existing Customers in the DCS program, the Successful Respondent shall collaborate with the MSI and other Service Component Providers to promote the Services to public sector entities within the State of Texas; including all potential DCS Customers, specifically State agencies, universities and higher education, counties, and municipalities.
- (b) Successful Respondent shall, at a minimum:
  - (i) Leverage the MSI-provided Outreach System and Customer Relationship Management system as agreed when executing its own marketing and advertising programs
  - (ii) Support the MSI in the creation and maintenance of its annual outreach plans aimed at increasing the DCS Customer base for the DCS Program, including but not limited to defining the effective outreach channels and developing material and collateral to support its Services.
  - (iii) Develop and execute against the Customer Outreach Plan, 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.
  - (iv) Coordinate evaluation of previous year's outreach plan achievement and DCS Customer growth through documentation of actual outreach achievements as compared to the previous year's plan.
  - (v) Collaborate with new and existing DCS Customers to understand their needs and to promote the benefits of DCS initiatives through thoughtful and cost-effective proposals following the Request for Solution process, which shall, at a minimum:
    - A. Communicate and promote specific service benefits to targeted needs;
    - B. Deliver compelling incentives to DCS Customers to use the Services; and

- C. Build trust through promotion of the benefits, such as ease of use, security, and privacy.
- (vi) Participate with the MSI, DCS Customers and other Service Component Providers in a community that shares knowledge, ideas, and best practices to collaborate and drive cost-effective innovation.
- (vii) For any new DCS Customer or expansion of existing DCS Customer's use of DCS services, the Successful Respondent shall align and support the MSI established on-boarding and request processes.
  - A. Include and participate in MSI and TSS Request for Solution processes including the use of solution architects and project managers, coordinating with TSS, MSI, DIR and other impacted SCPs in the development of comprehensive solution designs and project plans for the deployment of Customer and enterprise solutions.

## 9.8. Customer Satisfaction Surveys

- (a) The MSI will have responsibility for coordinating the development, maintenance, and execution of the surveys with DIR within the established Governance model. The MSI will develop the mechanism, facilitate responses, tabulate results and report results back to DIR and DCS Customers as part of an ongoing program for measuring customer satisfaction.
- (b) DIR will have overall review and approval of the customer satisfaction surveys, to include input and approval of the survey recipients, the survey methodology, and the survey questions.
- (c) The Successful Respondent shall work with the MSI in developing, delivering, reporting, and tracking customer satisfaction. The Service Component Providers shall support the MSI in accordance with the established SMM. See Critical Deliverable Annual Customer Satisfaction Improvement Plan for the description and acceptance criteria.

## 9.9. Service Management Requirements

- (a) DIR expects that the Successful Respondent follow design and implementation principles which will be, to the extent applicable, ITIL compatible. Successful Respondent shall align its design and delivery of services with ITIL concepts and techniques for managing the DCS public cloud and computing environment and integrate service management and reporting via the MSI operating model and systems. It is expected that Respondents identify where their service delivery model differs from the ITIL framework.
- (b) Respondents are advised that the DCS team and Customer-facing functions have been operating under and have been trained on ITIL principles and processes through the MSI's training program. Therefore, Respondents are not required to propose ITIL training as part of their response.
- (c) The Successful Respondent will design and implement the Service as to ensure the appropriate Service elements both integrate with and enable the areas:
- (d) The MSI Service Desk handles tier 1 support for incidents, problems and questions as well as providing an interface for other activities such as:
  - (i) Change requests;
  - (ii) Maintenance contracts;
  - (iii) Software licenses;
  - (iv) Service level management;
  - (v) Configuration management;
  - (vi) Availability management;

- (vii) Financial management;
- (viii) Application management; and
- (ix) IT Services continuity management.

### 9.9.1. Incident Management

(a) Successful Respondent shall, at a minimum:

- (i) 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.
  - (ii) 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.
  - (iii) Comply with MSI policies and procedures for Incident Management as documented in the SMM.
  - (iv) Coordinate with the MSI to develop and approve Successful Respondent-related Incident Management content in the MSI-managed SMM.
  - (v) Utilize the Incident Management System provided by the MSI for all information related to an Incident.
  - (vi) 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.
  - (vii) Resolve Incidents in accordance with the SMM, knowledge database documents, and configuration database(s).
  - (viii) Identify and classify Incident severity and handle according to agreed-upon Incident response procedures and assume end-to-end responsibility.
  - (ix) Escalate Incidents in accordance with the SMM, knowledge database documents, and configuration database(s).
  - (x) Provide tier 2 support and tier 3 support.
  - (xi) Support bringing technical resources and any third-party resources onto MSI led troubleshooting calls as needed and requested.
  - (xii) Participate in Incident review sessions.
  - (xiii) Update the progress of an Incident's resolution within the MSI tracking systems through to final closure.
  - (xiv) Verify that all records (e.g., inventory, asset and configuration management records) are updated to reflect completed and resolved Incidents.
  - (xv) Document solutions to resolved Incidents in MSI-managed central knowledge base. Accurately update all information pertinent to trouble ticket including general verbiage, codes, etc.
  - (xvi) 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.
  - (xvii) Conduct follow-up with DCS Customer representative who reported the Incident to verify the Incident was resolved to their satisfaction.
  - (xviii) 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.
- (b) 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.
- (c) The MSI shall provide the systems, processes, and service delivery oversight necessary to ensure consistent, quality service delivery.

### 9.9.2. Problem Management

The Successful Respondent shall, at a minimum:

- (i) Provide Problem Management Services in coordination with the MSI Problem Management structure to minimize the adverse impact of Incidents on DCS Customer's business operations.

- (ii) 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.
- (iii) Provide proactive Problem Management to identify and solve Problems and known errors before Incidents occur, including:
  - A. performing predictive analysis activities, where practical, to identify potential future Problems,
  - B. develop recommended mitigation plans, and
  - C. implement approved corrective mitigation actions and processes.
- (iv) Maintain, update, and disseminate information about Problems and the appropriate workarounds and resolutions to reduce the number and impact of Incidents.
- (v) 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 DCS Customer and other SCPs in performing their Problem Management functions related to the in-scope Services.
- (vi) 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.
- (vii) Coordinate with the MSI to develop and implement processes for Problem Management and root cause analysis (RCA).
- (viii) Comply with MSI policies for Problem Management and RCA.
- (ix) Participate in Problem Management review meetings.
- (x) Use and update the Problem Management knowledge database managed by the MSI.
- (xi) Perform Problem Management activities as set forth in the SMM.
- (xii) 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.).
- (xiii) 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.
- (xiv) 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.
- (xv) Identify, develop, document (in the MSI Problem Management tool), and recommend appropriate workarounds for known errors of unresolved Problems.
- (xvi) Create documentation with recommended corrective actions to resolve a Problem and submit to Change management for review and approval using the MSI provided tool.

### 9.9.3.Change Management

The Successful Respondent shall, at a minimum:

- (i) Perform Change Management Services utilizing standardized methods and procedures as defined in the SMM to provide efficient and prompt handling of all Changes.
- (ii) Assist DCS Customer in, DCS SCP, or MSI in creating the schedule for any Changes and implementing such Changes.
- (iii) Assist 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 DCS Customer requirements.
- (iv) Comply with MSI Change Management processes and training requirements as set forth in the SMM.
- (v) Review and approve refinements to Change Management processes and training requirements.
- (vi) Provide necessary information to DCS Customer, DCS SCP or MSI as required to assist in documenting all Request for Change's (RFCs), which could include Change cost, risk impact assessment, and system(s) security considerations.
- (vii) Coordinate with DCS Customer to assist in the development of a schedule of planned approved Changes.
- (viii) Perform maintenance during regular Maintenance Periods as defined in the SMM, or as scheduled in advance with the approval of DCS Customer, DCS SCPs or MSI as appropriate.

- (ix) Provide Change documentation, as required, to the MSI, including proposed metrics on how effectiveness of the Change might be measured.
- (x) As requested, participate in traditional or digital CAB meetings and workflow to review planned Changes and results of Changes made.
- (xi) 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 DCS Customer, DCS SCPs, or MSI as appropriate, in a way that minimizes risk exposure and maximizes availability of the Services.

#### 9.9.4. Configuration Management

- (a) The Successful Respondent will perform Configuration Management to 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 enable the Successful Respondent's Services. The MSI consolidates information from multiple Service Component Provider Configuration Management Databases (CMDBs) that contain details of CIs used in the provision, support, and management of IT services.
- (b) The Successful Respondent shall, at a minimum and as defined in the SMM:
  - (i) 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.
  - (ii) Integrate Successful Respondent's Configuration Management process with the MSI's Configuration Management process and systems, including providing Successful Respondent Configuration data electronically to MSI's Configuration Management System (CMS) / CMDB in the agreed data format.
  - (iii) Communicate and coordinate the Configuration Management processes and policies within its organization.
  - (iv) Actively cooperate in information exchange between and among the SCPs, MSI, DIR and DCS Customer to improve end-to-end Configuration Management.
  - (v) Work with the MSI to provide a complete Configuration Management audit trail to meet DIR and DCS Customer legislative and policy requirements.
  - (vi) Conform operations to policies and procedures that set the objectives, scope, and principles that ensure the success of the Configuration Management process.
  - (vii) Work with the MSI in establishing categorization and classification structures to ensure the proper documentation and maintenance of CIs.
  - (viii) 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.
  - (ix) Record all Successful Respondent's CI information including, but not limited to, equipment, software, services, and equipment.
  - (x) Verify that all CIs supporting the Successful Respondent's Services including Equipment, Software, and Services are incorporated into the CMDB.
  - (xi) Utilize the CMDB provided by the MSI as the single source of information regarding all CIs within Successful Respondent scope.
  - (xii) Ensure that all configuration data related to the Services resides in the CMDB.
  - (xiii) Integrate the Successful Respondent's other systems, including all appropriate and required licenses and/or interface with the MSI's Configuration Management System (CMS).
  - (xiv) Where Successful Respondent has an internal CMS, integrate that system with the MSI CMS as required.
  - (xv) Where Successful Respondent has an internal CMDB integrate that database with the MSI CMDB.
  - (xvi) Provide customization as required to enable the Configuration Management processes as defined in the SMM.
  - (xvii) 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.

- (xviii) Comply with existing and established SMM processes.
- (xix) Tracking changes to resources/services and their impact on associated resources.

#### 9.9.5.Capacity Management

- (a) Capacity Management assesses the current operations and future demands, pre-empting performance issues by taking the necessary actions before they occur.
- (b) The Successful Respondent shall, at a minimum:
  - (i) 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.
  - (ii) Project future supported service and compute-based trends and capacity requirements in conjunction with provided capacity usage reports, suggest new projects or efforts as it pertains to the Services;
  - (iii) Seek authorization to purchase additional capacity for any Service resource that has reached critical usage levels and is impacting Successful Respondent's ability to provide the Services;
  - (iv) Review supported scope compute, storage and Service performance and capacity and throughput for new applications and DCS Customer deployments before promotion into the production.
  - (v) Communicate and coordinate the Capacity Management processes and policies within Successful Respondent's organization.
  - (vi) Actively cooperate in information exchange between and among the SCPs, MSI, DIR and DCS Customer to improve end-to-end Capacity Management.
  - (vii) Provide the means to automatically aggregate resource and system performance, system utilization, capacity limits for Successful Respondent Services and provide electronically to the MSI in an agreed format and frequency.
  - (viii) Provide the means to automatically calculate and forecast Successful Respondent Services capacity requirements through trending of collected data anticipating capacity needs.
  - (ix) In an automated manner, aggregate capacity information including current capacity and utilization, trends, issues, and actions at the DCS Customer and Services level.
  - (x) Initiate Incident Management, Problem Management or Request Management activities as needed to address Capacity Management issues and trends.
  - (xi) Action and track agreed capacity mitigations through associated Incidents, service requests, changes or projects using the MSI provided systems.
  - (xii) Participate and contribute to Capacity Management meetings.
  - (xiii) Incorporate appropriate capacity modeling to extrapolate forecasts of growth and other changes in response to projected DCS Customer business and operational needs.
  - (xiv) Provide meaningful Capacity Planning input to the MSI-coordinated Capacity Plan.
  - (xv) Provide meaningful Capacity Planning input to the Technology Plan to develop requirements for long-range planning.
  - (xvi) Provide meaningful Capacity Planning input to the Refresh Plan to ensure Refresh and Technical Currency.

#### 9.9.6.Refresh and Technical Currency

- (a) The Successful Respondent will work with the MSI to ensure that refreshes are done as scheduled and technical currency is maintained in the Services. The Annual Technology Refresh Plan is required as a Critical Deliverable, as defined in **Attachment 1.1 Deliverables**.
- (b) Successful Respondent's responsibilities include:

- (i) Work with TSS, DCS SCPs, and DCS Customers to maintain application currency and ensure the service components align with the DCS standard services and software platforms as described in the DCS Standard Configurations.
- (ii) Upgrade and replace Equipment and Software (Refresh) as required in the Financial Responsibility Matrix throughout the Term, for purposes that include meeting DIR's and DCS 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.
- (iii) Cooperate and coordinate on-going Refresh activities with the full Refresh Program at the direction of the MSI and in alignment with DCS Customer application upgrade activity.
- (iv) Deploy Equipment and Software associated with any Refresh in accordance with the standards of DIR's technical architecture and the Technology Plan.
- (v) Accommodate the timeframes and other requirements associated with Refresh, as well as the financial responsibility for the underlying assets, as provided in the Financial Responsibility Matrix.
- (vi) 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.
- (vii) Cooperate, report, and support the management of Refresh Responsibilities by the MSI.
- (viii) Where the Successful Respondent is financially responsible for Equipment and Software used in conjunction with the Services, as listed in the Financial Responsibility Matrix, Successful Respondent's responsibilities include:
  - A. Refresh the assets during the Term, including responsibility for the assets, the implementation, and ongoing support.
  - B. At a minimum and/or in the absence of a defined Refresh timeframe, maintain technical currency in accordance with Industry Standards.
- (ix) Where DIR, SCPs or 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.
- (x) Regardless of the ownership of underlying assets, Successful Respondent responsibilities include:
  - A. 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.
  - B. Provide minimal disruption to DIR's and Customers' business operations associated with technology Refresh.
  - C. Use best practices and effective automation tools during Refresh deployment.
  - D. Perform all Changes to Equipment and Software in accordance with Change Management procedures.

### 9.9.7.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. Refresh includes both hardware age and software currency. Successful Respondent's responsibilities include:

- (i) Develop a continual plan for Refresh, including:
  - A. Within one-hundred and twenty (120) days prior to, and no less than 10 business days ahead of DIR's annual planning process meetings, review the 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.
  - B. Cooperate and participate in the planning activities led by the MSI.

- (ii) 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.
- (iii) For Successful Respondent-owned assets, Successful Respondent and DIR will mutually determine whether Successful Respondent will replace an asset and the appropriate replacement date.
- (iv) 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.
- (v) 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).
- (vi) 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.
- (vii) Adhere to DIR's approved plan, and execute that plan utilizing established procurement processes, to initiate refresh and retirement activities.
- (viii) Provide monthly reports 180 days prior to lease expiration date showing assets to be refreshed with latest data.
- (ix) Notify DIR monthly of all open agreements related to assets that are retired or will retire within 180 days of the report date.
- (x) Track and report on the completion progress of asset Refresh.
- (xi) Actively support TSS in workload assessment as part of refresh and annual technology planning.
- (xii) Update and archive asset records after retirement.

#### 9.9.8. Request Management and Fulfillment Requirements

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

##### 9.9.8.1. Request Management Processes

The Successful Respondent shall, at a minimum:

- (i) Actively participate with the MSI to develop and document processes.
- (ii) 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.
- (iii) Actively cooperate in information exchange between and among the Successful Respondent, the MSI, other Service Component Provider(s), DIR, and DCS Customer to improve end-to-end Request Management.
- (iv) Integrate the Successful Respondent's Request Management process with the MSI's Request Management process and systems, where the processes interact.
- (v) Facilitate the automation or mechanization of Service Requests between Successful Respondent, MSI, and other Service Component Provider(s) systems.
- (vi) Facilitate the transparency of Request Management through appropriate processes to provide a complete audit trail for the MSI to meet DIR and DCS Customer legislative and policy requirements.
- (vii) Communicate and coordinate the Request Management processes and policies within Successful Respondent's organization.
- (viii) Provide effective and agreed upon mechanisms for properly complying with the Request Management Policies.
- (ix) Actively participate in developing and establishing Request for Solution processes and appropriate mechanisms for rapid proposal development that provides a level of accuracy for budgetary information without requiring a full solution.

- (x) Actively work with the MSI in establishing processes and workflow for the proper routing of Service Requests.

#### 9.9.8.2. Service Request Operations

- (a) Actively work with the MSI as appropriate to ensure the proper exercise of Request Management activities across all functions and organizations that provide Services.
- (b) Actively participate in Service Request tracking efforts and provide and maintain regular communications between all parties and Authorized Users through Request fulfillment.
- (c) 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 DCS Customer and Authorized User satisfaction.
- (d) Work with 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 DCS Customer data.
- (e) Engage in effective Request Management governance process to enable the MSI and other SCPs in ensuring the following:
  - (i) 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.
  - (ii) 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).
  - (iii) Establish and continually maintain Authorized User lists on who is authorized to make Service Requests and type of requests they are entitled to make.
  - (iv) Communicate to DCS Customers the definition of Services, the Request Management processes, and changes thereto.
  - (v) Participate in regular training for Authorized Users on Request Management processes, Service definitions, and request mediums.
  - (vi) Perform regular collection of feedback from Authorized Users on the effectiveness of Request Management and engage in activities to improve process and service.
- (f) Enable multiple mediums for accepting Service Requests, including the Service Desk, Portal, Service Catalog and automated interfaces.
- (g) Enable the use of online self-service to allow Authorized Users to enter Service Requests from a pre-defined list of options.
- (h) Enable the provision for real-time visibility of data records associated with Service Requests.
- (i) Update required information on Service Requests within negotiated timeframes to provide an up-to-date accurate view of Service Requests.
- (j) Ensure proper approval, including financial authority, or the Service Request through automated means (where practical) prior to Service Request fulfillment.
- (k) 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.
- (l) The communications frequency shall be determined by the severity of the request and in compliance with the SMM.
- (m) Keep DCS 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.
- (n) Provide anticipated completion times for active Service Requests and update notification systems as required in the SMM to keep DCS Customers and Authorized Users informed in compliance with established Service Levels.
- (o) Work with the MSI to ensure consistent ownership of the Service Request from recording to completion.
- (p) 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.
- (q) Track the progress of fulfillment efforts and the status of all Service Requests, including:

- (i) Review the proposed fulfillment time for each Service Request with the appropriate party and update the status accordingly.
  - (ii) Provide regular updates on the status of all Service Requests within designated timeframes.
  - (iii) Coordinate Service Request tracking efforts and provide and maintain regular communications, per the SMM, between all parties and Authorized Users until Service Request completion.
  - (iv) Keep the DCS Customer and Authorized User informed of changes in Service Request status throughout the Service Request lifecycle in compliance with the SMM.
  - (v) Keep DCS Customer and Authorized Users informed of anticipated Service Request completion times for active Service Requests.
  - (vi) 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.
  - (vii) Track all Service Request completion against the original committed timeframe, regardless of any revisions.
- (r) Utilize the Request Management System provided by the MSI for all Request Management and Fulfillment activities.
  - (s) Provide for timely receipt and processing of all requests within designated timeframes from the Request Management System.
  - (t) Utilize and update the Request Management System with all relevant information relating to a Service Request.

### 9.9.8.3. Request for Solution (RFS)

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

- (i) Work with 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.
- (ii) Work with the MSI in developing and establishing RFS processes and appropriate mechanisms to ensure rapid proposal development that provides a level of accuracy for budgetary information without requiring a full solution (e.g., Rough Order Magnitude (ROM) pricing and high-level architecture).
- (iii) For all RFS delivered by the Successful Respondent only and that require no other SCP support:
  - A. Review RFS to validate for completeness.
  - B. Coordinate and lead meetings as required to review request, gather requirements, solution and develop the proposal.
  - C. Coordinate the attendance of all necessary subject matter experts in solution and requirement gathering sessions.
  - D. Provide a timeframe for delivering the solution proposal, including cost estimates, once requirements are complete.
  - E. Develop the solution which may include the technical solution, effort, acceptance criteria, solution design document, and pricing.
  - F. Ensure all solutions to requests conform to the DIR-approved architecture, standards, and pricing.
  - G. Ensure all solutions to requests conform the security policies, procedures, and guidelines of DIR.
  - H. Ensure all solutions to requests conform within the bounds and guidelines of DIR Shared Services technical guidelines.
  - I. Ensure all solutions to requests conform within the bounds and guidelines of the Contract.
  - J. Coordinate and facilitate solution reviews across the Successful Respondent as required to review and gain approval for the solution and pricing.

- K. Track all Project Change Requests in accordance with established procedures.
  - L. Provide a single proposal to requesting DCS Customer.
  - M. Iterate and adjust the solution and cost estimating template as required to adhere to the requesting DCS Customer's feedback and requirements.
  - N. Document DCS Customer approvals in accordance with established processes as per the SMM.
  - O. Gather and validate that the proposal acceptance comes from an appropriately authorized user.
  - P. Provide status to DIR and DCS Customers status of all outstanding requests such that DCS Customers can emphasize their organizational priorities.
  - Q. Initiate Project Management as appropriate upon proposal acceptance by DCS Customer.
- (iv) 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 TSS, the MSI, and the other SCPs as required to develop a coordinated DCS Customer solution, including executing 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).
- (v) Solution the Successful Respondent's portion of the RFS, including:
- A. Participate in meetings as required to review requests, gather requirements, solution, and develop proposals with other SCPs, DIR, DCS Customers, and other Third-Party Vendors.
  - B. Coordinate the attendance of all necessary Successful Respondent subject matter experts in solution and requirement gathering sessions.
  - C. Adhere to the TSS or MSI provided timeframe for delivering a solution proposal, including cost estimates, once requirements are complete.
  - D. Ensure all requests are solutioned within the DIR-approved architecture and standards and pricing.
  - E. Ensure all requests are solutioned within the security policies, procedures, and guidelines of DIR.
  - F. Ensure all requests are solutioned within the bounds and guidelines of DIR Shared Services technical guidelines.
  - G. Ensure all solutions to requests conform within the bounds and guidelines of the Contract.
  - H. Participate in solution reviews across the Successful Respondent and all affected SCPs as required to review and gain approval for the solution and pricing.
  - I. 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.
  - J. Tracking of all Project Change Requests in accordance with established procedures.
  - K. Work with TSS or the MSI in their development of a single proposal to the requesting DCS Customer.
  - L. Iterate and adjust solution and cost estimation as required to adhere to the requesting DCS Customer's feedback and requirements.
  - M. The Successful Respondent will conduct workload assessments to determine the best approach for solution design, and where Public Cloud may not be the best hosting strategy, identify such and work with TSS and SCP to ensure the optimum solution to meet Customers objective is developed.
  - N. Initiate Project Management activities, according to the SMM, upon proposal acceptance by DCS Customer.
  - O. Delivery of Solution Proposals and achieve the required SLA as defined in the below table, Attachment 1.2, Service Level Matrix and Attachment 1.3, Service Level Definitions and Performance Analytics, maintaining status and communications with the DCS Customer, the Successful Respondent, and SCPs. Successful Respondent will also coordinate and develop appropriate Operating Level Agreements with required SCP in support of defined service levels.

Complexity	Service Level (business days)
Simple	10
Medium	15
High	23
Custom	35

- (vi) Solution Complexity will be governed as defined in the following table and further defined within the approved SMM. Disposition of classification of requests will be performed by Successful Respondent.

**Table: Solution Complexity**

Description	Low Complexity	Medium Complexity	High Complexity	Custom Complexity
Technology Alignment (OS, DB, Middleware, etc)	Core	Core, Emerging, Declining	Emerging, Declining, Specialized	Specialized, Non-Standard Reference Architecture
Server Type	Virtual	Virtual	Physical	Physical
OS Instance Count	<5	>5 <=10	>10	>10
Install Location	ADC/SDC, Public Cloud	Non-Cons DC, Remote, Public Cloud	Non-Cons DC, Remote, Public Cloud, Hybrid	Hybrid
Multi-Application	No	No	Yes	Yes
DR Classification	5, 4	3	2, 1	1
Network Functions	Firewall – Int	Firewall – DMZ, Firewall - DMZ & Int	Firewall – EXT, DMZ & Int	Firewall – EXT, DMZ & Int
Project Type	Refresh of previous Demand, simple Public Cloud migrations	Application Rehosting, Refresh of previous Demand, medium complexity Public Cloud migrations	Application Replatform, Application Modernization, Cloud Assessment, Public Cloud Migration	Application Modernization, Facility Move, Public Cloud Migration

### 9.9.9.Asset Inventory and Management

- (a) 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 CIs) used in the provision, support, and management of IT services. Automated collection of asset and configuration data is a key component of the Service allowing for real-time reporting and management of DCS components.

(b) Successful Respondent responsibilities include:

- (i) 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.
- (ii) 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.
- (iii) Provide automation for all integration with the MSI's Asset Inventory and Management process and systems inclusive of auto-discovery functions to ensure real-time reporting of DCS infrastructure components.
- (iv) Communicate and coordinate the Asset Inventory and Management processes and policies within Successful Respondent's organization.
- (v) Actively cooperate in information exchange between and among the SCPs, MSI, DIR and DCS Customer to improve end-to-end Asset Inventory and Management.
- (vi) Work with the MSI to provide a complete Asset Inventory and Management audit trail to meet DIR and DCS Customer legislative and policy requirements.
- (vii) Conform operations to policies and procedures that set the objectives, scope, and principles that ensure the success of the Asset Inventory and Management process.
- (viii) Work with the MSI in establishing categorization and classification structures to ensure the proper documentation and maintenance of CIs.
- (ix) 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.
- (x) Record the CI information for Equipment, Applications, Software and Services.
- (xi) Verify that all CIs for the Equipment, Applications, Software, and Services are incorporated into the AIMS.
- (xii) Utilize the AIMS provided by the MSI as the single source of information regarding all CIs within Successful Respondent scope.
- (xiii) Ensure that all CI data related to the Services resides in the AIMS.
- (xiv) Integrate the Successful Respondent's other systems, including all appropriate and required licenses and/or interfaces with the MSI's AIMS.
- (xv) Where Successful Respondent has an internal asset inventory system or database, integrate that system or database with the MSI AIMS as required.
- (xvi) Provide customization as required to enable the Asset Inventory and Management processes as defined in the SMM.
- (xvii) 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.
- (xviii) Comply with existing and established SMM processes.

#### 9.9.10. IT Service Desk Requirements

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

(b) 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 DCS Customers' IT Services.

(c) The Successful Respondent shall, at a minimum:

- (i) Actively participate with the MSI to develop and document processes.
- (ii) Integrate Successful Respondent's Service processes with the Service Desk processes of the MSI, DCS Customer, and authorized Third Party Vendor(s), where the processes interact.
- (iii) Actively work with the MSI to assure the proper application of Service Desk across all functions and organizations that provide services to DCS Customers.
- (iv) Communicate and coordinate the Service Desk processes and policies within Successful Respondent's own organization and DCS Customers.
- (v) 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.
- (vi) Provide effective and agreed upon mechanisms for properly complying with the Service Desk policies.
- (vii) Manage all Incidents, Service Requests, etc., from Authorized Users relating to Services, including the following:
  - A. Assigning categorization and prioritization codes.
  - B. 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.
  - C. Closing all resolved Incidents, Service Requests, and other calls.
- (viii) 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.
- (ix) 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.
- (x) Analyze Incident trends and recommend and implement actions, with DIR and DCS Customer(s) approval, to reduce Incidents.
- (xi) Provide on-line FAQs and help documentation for common problems.
- (xii) Provide the MSI with information necessary to keep Authorized Users regularly updated with alerts advising of any new or changed information.

#### 9.9.11. Information Security Management Requirements

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. The Successful Respondent will coordinate with the MSI and the Security Operations SCP to develop an Annual Security Plan for in-scope Services. This plan is a Critical Deliverable, defined in **Attachment 1.1 Deliverables**.

##### 9.9.11.1. Information Security Management General Requirements

The Successful Respondent shall, at a minimum:

- (i) Work with the MSI and Security SCP in support of the overall cybersecurity risk management program.
- (ii) Work with the MSI and Security SCP to develop and maintain security procedures and Service Responsibility Matrices, physical and logical access strategies, and standards.

**State of Texas** Department of Information Resources, Data Center Services

- (iii) Adhere to the Information Security Management processes as defined in the SMM.
- (iv) Work with the MSI and Security SCP 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 and Security Operations SCP as required to enable these capabilities.
- (v) Implement security capabilities as required to achieve compliance with security laws, rules and regulations.
- (vi) Participate in security evaluations, as directed by DIR or requested by participating clients, which include conducting internal audits, supporting external audits, conducting self-assessments, and evaluating security Incidents.
- (vii) Participate in 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 or at such time as otherwise mutually agreed upon.
- (viii) Meet all Security-related deliverables and Performance Analytics which are to be agreed to by DIR and Successful Respondent.
- (ix) As requested, attend and contribute to Security Management and Risk Management meetings.
- (x) Resolve agreed actions and activities resulting from Security Management meetings.
- (xi) Work with the MSI and Security SCP to contribute to the creation and maintenance of a Security Plan across the Successful Respondent's Services
- (xii) Execute Successful Respondent's Security Plan which is agreed to by DIR and coordinated by the MSI.
- (xiii) Ensure that certificates for Successful Respondent's staff are kept current and report the status to the MSI on a quarterly basis.
- (xiv) Provide for vulnerability scans for all Successful Respondent 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.
- (xv) Provide a forward-looking schedule for the planned Successful Respondent Security testing, assessments and analysis.
- (xvi) In coordination with the Security SCP, participate in the evaluation of new technologies/capabilities for improving security and perform activities and/or solutions to address shortfalls in Security.
- (xvii) Where investment decisions are required, work with the MSI in providing options with associated costs and benefits for DIR review and approval.
- (xviii) In coordination with the Security SCP, 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.
- (xix) Work with the Security SCP and execute processes and according to the governance-approved Master Security Baseline Configuration (MSBC).
- (xx) Execute quarterly MSBC Health Checks and run scans quarterly that will feed baseline information to the Security SCP for the Security SCP to determine the health check of the systems.

#### 9.9.11.2. Security Regulations

(a) The Successful Respondent shall, at a minimum:

- (i) Adhere to the then-current safety and security policies, rules, procedures and regulations established by the State and DIR, and each DCS Customer with respect to such DCS Customer's data and facilities.
- (ii) Adhere to DIR and DCS Customer's then-current "Security Rules," as published in Chapter 202, Information Security Standards of the Texas Administrative Code.
- (iii) Comply with all security incident notification and response procedures as specified in the Service Management Manual.
- (iv) Comply with the policies defined by the FBI Criminal Justice Information Services (CJIS) requirements.
- (v) The Successful Respondent shall perform the Services in compliance with all federal and state laws and industry standards as they may be updated from time-to-time, including but not limited to the following:
  - A. *1 Texas Administrative Code (TAC) Chapter 202. TAC 202 provides the State of Texas security standards policies applicable to all Texas state agencies.*

**State of Texas** Department of Information Resources, Data Center Services

- B. *HIPAA – Health Insurance Portability and Accountability Act Privacy and Security Rules*
- C. *HITECH – Health Information Technology for Economic and Clinical Health Act*
- D. *FIPS 140-2 Federal Information Processing Standards Publication, Security Requirements for Cryptographic Modules*
- E. *FISMA – Federal Information Security Management Act*
- F. *FERPA – Family Educational Rights and Privacy Act*
- G. *IRS Pub 1075 – Tax Information Security Guidelines for Federal, State and Local Agencies*
- H. *PCI – Payment Card Industry Security Standards*
- I. *ISO/IEC 27001:2005 - Information technology – Security techniques – Information security management*
- J. *ISO/IEC 27002 – code of practice for information security management*
- K. *NIST 800 – National Institute of Standards and Technology standards and related publications*
- L. *CJIS Security Policy - FBI Criminal Justice Information System Security Policy and CJIS Security Addendum*

(b) DIR and DCS Customers comply with National Institute of Standards and Technology (NIST) Federal standards and related NIST 800 series Special Publications (SP) and Federal Information Processing Standards (FIPS) standards. Where there is a conflict between NIST, FIPS and 1 TAC Chapter 202 rules and security controls, the 1 TAC Chapter 202 takes precedence.

#### 9.9.11.3. Security Incident Management

The Successful Respondent shall, at a minimum:

- (i) Work with the MSI and Security SCP and contribute to the creation of a Security Incident Management process across the Successful Respondent’s Services.
- (ii) Provide plans and exceptions for Security Incident Management including Security Incident severity matrix, notification rosters, communications plans, and procedures for managing Security Incidents.
- (iii) Implement the Successful Respondent’s portion of the Security Incident Management process in concert with participation from the MSI and required Service Component Providers and DCS Customer personnel.
- (iv) Coordinate Security Incident Management procedures with Major Incident Management procedures.
- (v) Adhere to the Security Incident handling and notification processes that follow current NIST guidelines and is defined in the SMM.
- (vi) As required, implement, and maintain monitoring and alerting services that integrate into the MSI Incident Management System and Security SIEM for automated alert notification.
- (vii) Promptly investigate, document, and report security incidents in accordance with 1 TAC Chapter 202 and the SMMs.
- (viii) According to the defined processes, promptly communicate and escalate security Incidents to the MSI, Security provider, DCS Customer, and DIR.
- (ix) Conduct Root Cause Analysis and if necessary, develop and implement formal corrective actions or remediation plans once approved by DIR and the appropriate DCS Customer. Evaluate the analysis and proposed corrective actions to ensure future risks are adequately mitigated.
- (x) Provide Incident investigation and initiate corrective actions to minimize and prevent security breaches.

#### 9.9.11.4. Security Assessments

(a) 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.

(b) The following applies to Assessments in general:

- (i) 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.
  - (ii) 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”).
  - (iii) The Successful Respondent shall cooperate fully with DIR and/or the Security Assessment Company and provide 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 DCS Customers.
  - (iv) 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.
  - (v) 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 present to DIR 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.
- (c) The Parties shall cooperate with the utmost good faith to reach reasonable and timely agreements on such further definition and clarification and agree that such further definitions and clarifications shall in all respects be consistent with the terms of the security assessment requirements in this Exhibit. In addition, to the extent that a security assessment company reasonably establishes that certain definitions, procedures and methodologies are widely used in security assessments, the Parties agree to generally rely on the security assessment company’s definitions, procedures, and methodologies for guidance in reaching agreement. The Parties acknowledge that in reaching the final results of a security assessment, the security assessment company will be required to exercise its professional judgment and discretion in certain matters and, assuming such judgments are within established industry practices for security assessments, the Parties will defer to the conclusions of the security assessment company.
- (d) Successful Respondent acknowledges that DIR views the right to conduct Assessments as a critical inducement to DIR’s agreement to many of the terms of this Agreement, including the Term and termination rights provided for in the Agreement, and therefore Successful Respondent agrees that it will cooperate in good faith to accomplish the objectives contemplated by the security assessment for the benefit of DIR.

#### 9.9.12. Software License Renewal Management

Successful Respondent has responsibility for:

- (i) Working with 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:
- (ii) Comply with the Software License Renewal Management processes, as defined in the SMM.
- (iii) 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).
- (iv) In conjunction with the MSI, monitor Software License Renewal progress and SLA achievement.

- (v) Working with the MSI to ensure the requests and Change Requests are completed and closed upon renewal completion.
- (vi) Successful Respondent will update the contract data in the approved Software License Renewal System, coordinate with the DCS 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.

#### 9.9.12.1. Software License Compliance Management

The Successful Respondent will:

- (i) Work with the MSI to determine the compliance position, based on automated monitoring and reporting of 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:
  - A. For Successful Respondent provided and managed software, execute assigned Software License Compliance Management activities as defined in the SMM.
  - B. For DIR and DCS Customer-retained Software, track and maintain the applicable licensing and use information received from DCS Customers.
- (ii) 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.
- (iii) Monitor the Equipment for the presence of any unauthorized or non-standard Software.
- (iv) Define and check for particular Software signatures.
- (v) Check the presence and version of Software installed on a particular device and record in the MSI Asset Inventory and Management system.
- (vi) Provide reporting of license information and compliance to the MSI, at least quarterly or as directed by DIR.
- (vii) Store and track Software license agreements and associated license keys, including processes and procedures for renewals.
- (viii) Track license counts and associations within the MSI-provided CMDB.
- (ix) Collect and maintain the Contract and Proof of Entitlement (POE) within the MSI-provided system.
- (x) Work with the MSI to collect and normalize software titles to standard names.
- (xi) Work with the MSI to review the Software License Compliance position and determine appropriate remediation.
- (xii) Take ownership of assigned actions through the Incident, Request, Change, and Project processes for any reported non-compliance of software purchased versus software installed.
- (xiii) Provide clarifications about information presented in the Compliance Report to eliminate discrepancies.
- (xiv) Enable the use of Successful Respondent provided and managed Software to maintain strict compliance, including but not limited to:
  - A. Immediately notify and advise MSI of all Software license compliance issues associated with Services.
  - B. Enable 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, DCS Customers, or MSI.
  - C. Schedule, apply, and support security certificates used to secure confidential sessions (SSL) for Internet and Intranet transactions and communications as required by DIR or DCS Customers.
  - D. Coordinate and advise DCS Customers regarding certificates that are embedded in Applications.
  - E. Notify and advise DCS Customers of renewals regarding certificates in timely manner.

- (xv) Work with 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.
- (xvi) Work with the MSI in reporting of license information and compliance to DIR.

#### 9.9.12.2. Software Patch Management

The Successful Respondent shall, at a minimum:

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

#### 9.9.13. IT Service Continuity Management Requirements

- (a) 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 DCS Customers.
- (b) The Successful Respondent shall, at a minimum:
  - (i) 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, DCS Customer Service Location, or other Successful Respondent Facilities.
  - (ii) The DRPs and TRGs should comply with all applicable Federal and State requirements.
  - (iii) 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 this Exhibit.
  - (iv) Coordinate Successful Respondent's ITSCM plan with MSI ITSCM plans and DCS Customer Business Continuity Plan (BCPs) to ensure DCS 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.
  - (v) In the event of a service disruption, coordinate all ITSCM efforts to ensure smooth and efficient resumption of Services.

#### 9.9.14. Crisis Management

The Successful Respondent will perform Crisis Management as 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:

- (i) Following MSI, DIR, and DCS 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.
- (ii) Following statewide notification pyramid alert support as documented in the applicable business continuity plan.
- (iii) Coordinate with MSI, DIR, and DCS Customers requirements for Services that are critical to designated DCS Customer emergency management responsibilities.
- (iv) Coordinate with MSI, DIR, and DCS Customer regarding variances in Services as a result of Crisis Management in compliance with all SMM procedures.

#### 9.9.15. Release Management

- (a) The purpose of Release Management is to build, test and deliver specified Services that will accomplish the stakeholders' requirements and deliver the intended objectives.
- (b) The Successful Respondent shall, at a minimum:
  - (i) Work with the MSI and other SCPs 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.
  - (ii) Conform Successful Respondent operations to the agreed Release policies, processes and procedures as defined in the SMM.
  - (iii) Execute releases according to the approved Release Management methodology as defined in the SMM.
  - (iv) Use the MSI provided Release Management System as the single source of Release Management and information regarding all Successful Respondent Releases.

#### 9.9.16. Project Management

- (a) Project Management provides a way to execute and manage projects with the goal of delivering projects from request through completion, meeting DCS Customer requirements in terms of timing, quality, and cost.
- (b) The Successful Respondent shall, at a minimum:
  - (i) Be responsible for executing and managing projects related to the Successful Respondent's Services.
  - (ii) Conform Successful Respondent operations to MSI-defined policies and procedures as documented in the SMM to ensure the success of the Project Management process.
  - (iii) Use the MSI provided Project and Program Management (PPM) system as the single source of project management and information regarding all projects and programs.
  - (iv) Ensure that all Successful Respondent Project Management data resides in the PPM system.
  - (v) Execute projects according to the approved Program Management and Project Management methodology as defined in the SMM.
  - (vi) 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:
    - A. Adhere to the requirements and guidelines as outlined in the Project Delivery Framework located on the DIR website. The link currently resides here: <https://dir.texas.gov/View-Resources/Pages/Content.aspx?id=16>.
    - B. Provide project deliverables as required for the QAT to review and provide proactive monitoring of project outcomes.

- C. Develop and execute corrective action plans for projects with QAT identified project risks.
  - D. Provide status reports to the MSI and DIR as required to report to QAT stakeholders (state leadership, DIR leadership, DIR and MSI project teams).
  - E. Escalate significant issues to the MSI and DIR and advise on alternative methods for correction.
- (vii) The Successful Respondent is responsible for providing technical project management necessary to support the TSS or MSI project manager to ensure customer projects are accurately delivered on schedule. The Successful Respondent will follow the SMM process and leverage MSI toolsets provided to:
- A. Follow established Project Management processes as documented in the SMM; and
  - B. Use the MSI Project and Program Management system for all project activity.
  - C. The Successful Respondent will, in conjunction with the delivery of any project that can adversely impact the operation of any DCS Customer or SCP, include the following project quality assurance services. The Successful Respondent will:
  - D. Develop and document quality assurance processes and procedures for the delivery of Services to DCS Customers.
  - E. Confirm compliance with agreed-upon quality assurance procedures.
  - F. Conduct quality and progress reviews with appropriate DIR and/or DCS Customer personnel.

## 9.10. Business Management

### 9.10.1. Operational Intelligence

- (a) Successful Respondent shall provide the data to the MSI via automated API integration for report creation and posting via the MSI-managed Operational Intelligence System and Portal as specified in **Appendix A Reports** and Service Level reports as defined in Service Levels.
- (b) The Successful Respondent shall, at a minimum:
- (i) Provide automated data feeds as agreed (e.g., format, timing, delivery mechanism) by the MSI to allow the MSI to generate reporting for all Successful Respondent reports identified as being presented through the MSI systems.
  - (ii) For those reports agreed to be provided by the Successful Respondent, provide online reporting capability with near real-time data for use by DCS.
  - (iii) As agreed with DIR, coordinate with the MSI to provide single sign-on access to Successful Respondent's reports through the MSI Portal.
  - (iv) As appropriate, provide near real-time operational data feeds to the MSI-managed Operational Intelligence System.
  - (v) Provide on-time, monthly service-level performance data for each Service Level requirement, to the MSI-managed Service Level Management System.
  - (vi) Provide mutually agreed upon reports and data to the MSI to enable invoice reconciliation.
  - (vii) Coordinate with the MSI and provide data to enable the creation of integrated performance dashboards. Dashboard data should provide:
    - A. Near real-time health dashboards for any Systems managed by Successful Respondent highlighting status of health metrics as defined by DCS Customer.

- B. Report monthly, quarterly, and annually in the Security Dashboard on the deployment of Tools and procedures to the DCS Customer Environment.
- (viii) 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.
- (ix) As required, collaborate with other DCS SCPs, to include sharing reports and information via the MSI Portal or other mutually agreed upon mechanism as appropriate to ensure effective Service delivery.
- (x) Enable integration of applicable security Service solutions, in which data from multiple sources (e.g., scan results, multiple IDS platforms/IPS devices, and Master Data Services (MDS) devices) are incorporated and integrated into the Service.
- (xi) 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.

### 9.10.2. Service Level Management

- (a) Service Level Management includes the activities associated with managing and reporting attainment of Service Level performance, deliverable commitments, and customer satisfaction.
- (b) The Successful Respondent shall, at a minimum:
  - (i) Provide accurate and timely SLA data to the MSI as defined in Article 6 [Performance Model and Service Level Management](#), and the SMM to the MSI-managed Service Level Management System as agreed with the MSI (e.g., format, timing, delivery mechanism).
  - (ii) When SLAs fail to meet minimum or expected Service Level targets, implement Service Level Improvement Plans (SLIP), as described in the SMM.
  - (iii) Analyze DCS Customer Scorecard feedback to understand DCS Customer issues and develop and execute issue resolutions.
  - (iv) 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.
  - (v) Develop an action plan to address suggested improvements to the Services identified by Successful Respondent and DCS Customer, including the following:
    - A. Provide the action plan to DCS Customer for review.
    - B. Implement DCS Customer-approved action plans.
    - C. Report in the Dashboard on progress and improvements made on approved action plans.
  - (vi) Summarize and report on plans and activities that affect the overall Services to MSI and DIR governance boards.

### 9.10.3. IT Financial Management

Successful Respondent must provide automated IT Financial Management Services via API. The Successful Respondent shall, at a minimum:

- (i) Actively work with the MSI to develop and document IT Financial Management processes.
- (ii) Actively cooperate in information exchange between and among the MSI, DIR, and DCS Customer to improve end-to-end IT Financial Management.
- (iii) 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.
- (iv) 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.

- (v) Actively work with the MSI to assure the proper application of IT Financial Management across all functions and organizations that provide services to DCS Customers.
- (vi) Communicate and coordinate the IT Financial Management processes and policies within Successful Respondent's own organization.
- (vii) 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.
- (viii) Integrate Successful Respondents' systems and chargeback data with the MSI IT Financial System, including providing all appropriate and required licenses and/or interfaces.
- (ix) Provide sufficient data and detail to support DIR, DCS Customers, State and Federal funding accounting, grant, and audit requirements.
- (x) Collect, aggregate, and provide billing, service provisioning, and service metric information to the MSI as required.
- (xi) Identify unique DCS Customer account identifiers to identify Applications, Application Instances, and other service information as required.
- (xii) Provide the MSI with monthly invoice data required for the MSI to render the Successful Respondent statement of Services.
- (xiii) Support all charges with detailed invoice data as required, and supporting utilization data at the DCS Customer, Resource Unit, Charge Category (e.g., Programs, Divisions, Organization Units) as required by the MSI.
- (xiv) Actively participate in developing and maintaining the processes for the resolution of invoice disputes within designated timeframes.
- (xv) Provide effective and agreed mechanisms for crediting DCS Customers as appropriate.
- (xvi) Effectively execute the processes to record, track, and manage incidents of invoice disputes.
- (xvii) Research and review invoice disputes for completeness and ensuring data accuracy, and, when necessary, request clarifying data from DCS Customer.
- (xviii) Initiate additional treatment of invoice disputes to facilitate resolution within designated timeframes.
- (xix) Ensure that incidents of invoice disputes are continually updated, at a minimum on a weekly basis.
- (xx) Keep the MSI informed of activity and anticipated resolution times for active incidents of invoice disputes.
- (xxi) Allow DIR to monitor and validate invoice dispute process on an ongoing basis.
- (xxii) Provide a process for escalating to Successful Respondent management incidents of invoice disputes not resolved within the time frames established within DIR policies.
- (xxiii) Provide data to enable the MSI to report on all DCS financial items, including, at a minimum:
  - A. Provide application transaction and financial transaction data to the MSI to enable the MSI provided Financial Management System functionality to allow for near real-time reporting of the DCS transaction and payment details including reports as required to fully reconcile all attempted and failed transactions.
  - B. Provide Customer, application, and transaction data to the MSI as required to enable the MSI provided reporting on transactions and payment data by type of transaction, application, Customer, etc.
  - C. Provide the required data to the MSI with the appropriate level of detail to enable the MSI to link all financial items to each individual transaction.
  - D. Provide the required data to the MSI to enable the MSI to invoice DCS Customers for DCS fees.

## 10. Contract Management

### 10.1. Contract Changes

- (a) Any change or modification to the Agreement that alters pricing, the material terms of the Agreement, or alters Articles 1 through 14 of the Agreement must be made by a properly executed Contract amendment.
- (b) Other changes or modifications to the Agreement may be made through the appropriate contract change process and shall occur in accordance with the relevant SMM.

### 10.2. Deliverables

- (a) Deliverable: a vendor-provided tangible item or outcome that DIR reviews and approves at a specified date/frequency during the term of the contract, excluding reports that are managed/monitored through other defined processes.
- (b) Deliverables may have certain attributes that impact the review and acceptance.
- (c) The attributes for each of the deliverables are detailed in **Attachment 1.1 Deliverables** and summarized below.
- (d) Critical (C) (flagged within the Agreement and referenced in **Attachment 1.1 Deliverables**). Deliverables that are Critical have associated Deliverable Credits payable to DIR in the event Successful Respondent fails to successfully **complete and submit such Deliverables to DIR on or before the due dates identified in Attachment 1.1**. For further clarity, successfulness is measured by whether the Deliverables meet the associated Acceptance Criteria.
- (e) Payment (P) Payment Deliverables are the deliverables that have associated payments due to the Successful Respondent after DIR approval of such deliverables. Payment will be provided in accordance with **Exhibit 2 Pricing**.
- (f) Time-critical (T) – Deliverables that are designated as time-critical will have an expedited review period of five (5) Business Days.
- (g) For avoidance of doubt, a specific Deliverable’s attributes may be changed upon mutual agreement and through the appropriate contract change request process as determined by the material nature of changes.
- (h) Project Milestones. Project milestones are those produced and delivered as part of a Request for Service process and are specific to a project being delivered. DIR or DCS Customers shall have the right to review and accept or reject the milestones in accordance with the SMM.

### 10.3. Deliverable Acceptance Criteria

- (a) In order to eliminate the potential for frequent submission and rejection of Deliverables, the Successful Respondent shall meet with DIR and reach agreement on the construct and content for Deliverables prior to creation. The Successful Respondent shall coordinate fully and appropriately with DIR and its partners throughout the development of Deliverables and reviews of deliverables prior to formal submission as

requested. At a minimum, Deliverables shall meet the acceptance criteria defined in **Attachment 1.1 Deliverables**. Unless otherwise agreed, and as applicable, Successful Respondent shall perform comprehensive testing (e.g., unit, string, integration, stress, volume, system testing) on each such Deliverable prior to submitting such item to DIR for Acceptance. DIR considers the Deliverable due date to be the day by which the Deliverable is ready for acceptance and formally submitted.

- (b) The Successful Respondent shall use the SMM process to formally submit final versions of the Deliverables to DIR.
  - (i) For all Deliverables, the Successful Respondent shall comply with the following requirements:
  - (ii) The Successful Respondent shall follow all DIR-prescribed processes and procedures and SMMs;
  - (iii) The Successful Respondent shall provide actionable Deliverables which successfully meet all requirements outlined in the Agreement;
  - (iv) The Successful Respondent shall deliver all Deliverables in accordance with the DIR-approved Deliverable schedule;
  - (v) The Successful Respondent shall correct any latent defects identified after the acceptance of a Deliverable at no additional cost to DIR;
  - (vi) The Successful Respondent shall comply with specific acceptance criteria detailed in the Agreement and referenced in **Attachment 1.1 Deliverables**.

#### **10.4. Deliverable Expectation Document (DED)**

- (a) At DIR's discretion, a DED may be used for Deliverables to document mutually agreed upon Deliverable descriptions, applicable standards, and more clearly define Acceptance Criteria previously documented in **Attachment 1.1 Deliverables**. The Successful Respondent and DIR will develop and mutually agree on DEDs. Deliverable acceptance will be contingent on material compliance with the DED and any rejection of a Deliverable must be accompanied by a description of the material non-compliance with the DED. DIR, in its sole discretion, may choose to forgo the creation of the DED.
- (b) The DEDs shall not contradict nor alter the Contract Acceptance Criteria requirements set forth in the Agreement or in **Attachment 1.1 Deliverables**. In the absence of a DED, the Acceptance Criteria for a Deliverable would be material compliance with the requirements as set forth in the Agreement or in **Attachment 1.1 Deliverables**.
- (c) There may be situations where agile development of deliverables may be appropriate. In such cases, the Acceptance Criteria in **Attachment 1.1 Deliverables**, for a Deliverable may be described at a high level and the DED may be used to capture requirements for a sprint or series of sprints.
- (d) Any changes to the DED will be approved through mutual agreement between DIR and the Successful Respondent.
- (e) The following requirements may be documented in the DEDs:
  - (i) Format of the Deliverables;

- (ii) Deliverable Description;
- (iii) Submission Process and Requirements;
- (iv) Delivery Schedule including Incremental Delivery Dates, if applicable;
- (v) Review and Comment Requirements (who, when, how); and
- (vi) Acceptance Criteria.

### 10.5. Deliverables Review Meeting

The status of each Deliverable and any associated issues will be managed through a Deliverables review meeting between DIR and the Successful Respondent. The objective of the meeting is to review the status of Deliverables, communicate Deliverable owners and Deliverable recipients for upcoming Deliverables, review non-compliant deliverables and remediation plans for those Deliverables as needed.

### 10.6. Acceptance Review Period

- (a) It is critical to the success of the Successful Respondent that the deliverable acceptance process is thorough and that any deficiencies are addressed as early as possible to minimize impacts to the Services. Designated DIR working teams will be reviewing the Deliverables throughout the phases of development. Successful Respondent will solicit input from DIR as the Deliverables are developed. The Successful Respondent shall review the expectations in advance so as to obtain acceptance of the final Deliverable within the Acceptance Review Period. Feedback and suggestions received from DIR will be incorporated into the Deliverable.
- (b) There may be deliverables within the Agreement that are designated to have a “parent/child” relationship with another Service Component Provider. For those specific deliverables, the review and acceptance periods will follow the deliverable designated as the “parent” deliverable.
- (c) DIR will notify the Successful Respondent, in writing, within ten (10) Business Days, or such other time as may be mutually agreed to considering the size, criticality, and complexity of the Deliverable, or as may be designated as Time-Critical (TC) in **Attachment 1.1 Deliverables**, of the acceptance or non-acceptance of the Deliverable. During this Acceptance Review Period, DIR shall review and may further test each Deliverable, individually and/or collectively, to determine whether such item(s) comply with Acceptance criteria. Successful Respondent shall cooperate with such review and testing efforts, provide a technical environment to facilitate such review, and provide all applicable documentation that may assist in such review and testing. DIR will notify the Successful Respondent, any deficiencies that must be corrected prior to acceptance.
- (d) If the Successful Respondent does not receive written notice from DIR by the end of the review period, the Successful Respondent may notify DIR in writing that DIR has five (5) additional Business Days to provide written notice. The Deliverable will be deemed to be accepted by DIR if DIR does not provide such notice of acceptance or non-acceptance at the end of this additional five (5) Business Day period.
- (e) If DIR does not provide notice of Acceptance or deliver a notice of Noncompliance to Successful Respondent by the end of the Acceptance Review Period, DIR may request in writing an additional Acceptance Review Period to be mutually agreed to by both parties. Should DIR require additional time to review the Deliverable and has not received notice from the Successful Respondent regarding the additional Acceptance Review

Period of five (5) Business Days, DIR may provide notice to the Successful Respondent that an extension of the DIR review period is needed. Successful Respondent and DIR shall work together to establish a revised acceptance review period.

- (f) Neither DIR's nor any DCS Customer's use in a live production environment shall constitute Acceptance, affect any rights and remedies that may be available to DIR or a DCS Customer, and/or constitute or result in "acceptance" under general contract Laws, the State's Uniform Commercial Code or any other Laws.

#### **10.7. Noncompliance**

- (a) If DIR delivers to the Successful Respondent a written notice of non-compliance, the Successful Respondent shall correct all deficiencies identified in DIR's notice and within five (5) Business Days for written Deliverables, or such other time as mutually agreed to, at no additional charge to DIR. Beginning upon receipt of notice from Successful Respondent that the Deliverable resubmission is ready to be Accepted, an Acceptance Review Period of ten (10) Business Days shall begin again and the Parties shall perform their obligations as described above in Acceptance Review Period.
- (b) For deliverables that are Time-Critical as designated in **Attachment 1.1 Deliverables**, within two (2) Business Days or as otherwise mutually agreed, after receiving such notice from DIR, and at no charge to DIR, Successful Respondent shall correct such Noncompliance, satisfy the Acceptance Criteria as outlined in the Noncompliance notification. Beginning upon receipt of notice from Successful Respondent that a Deliverable resubmission is ready to be Accepted, an Acceptance Review Period of two (2) Business Days or as otherwise mutually agreed, shall begin and the Parties shall perform their obligations under Section [10.6 Acceptance Review Period](#) above.

#### **10.8. Failure to Cure a Noncompliance**

- (a) If Successful Respondent (1) requires more than two (2) attempts to cure a particular Noncompliance; (2) does not correct a Noncompliance within the timeframes defined in the Section [10.6 Acceptance Review Period](#); or (3) cures a particular Noncompliance and such cure results in another Noncompliance and Successful Respondent is not able to collectively cure such Noncompliance(s) within one (1) attempt in five (5) Business Days, then DIR may, in its sole discretion, apply any remedies including, but not limited to Deliverable Credits.
- (b) After pursuing the cure process stated above, upon written notification to Successful Respondent, DIR in its sole discretion may choose to forgo assessing any remedies, including but not limited to Deliverables Credits and may choose to:
  - (i) conditionally Accept the Deliverable and require Successful Respondent to develop a remediation plan, subject to DIR's acceptance and within time frames reasonably requested by DIR whereby Successful Respondent shall design and implement a workaround solution that mitigates the Noncompliance;

- (ii) correct the Noncompliance itself or hire a third party to correct the Noncompliance at Successful Respondent's expense (all such out-of-pocket expenses and costs of DIR and/or the DCS Customer to be subject to set-off as set forth in **Exhibit 2 Pricing** requirements related to Set Off);
  - (iii) implement and use the Deliverable despite the Noncompliance and equitably reduce the Charges; and/or
  - (iv) exercise any of its other rights under this Agreement or available at law or in equity.
- (c) The remedies above are in addition to and shall not limit DIR's other remedies, whether at Law, in equity, or under this Agreement.

#### **10.9. Remediation of Defects in Previously Accepted Items**

- (a) In the event of a discovery of a latent defect in a previously Accepted Deliverable or other Deliverable, where such latent defect would have qualified as a Noncompliance at the time of Acceptance, upon discovery, the Successful Respondent will, at no additional charge, repair or replace or otherwise correct the Noncompliance to the level of performance specified in the Agreement.
- (b) Further, should any modification or rework of a previously Accepted Deliverable or other Deliverable be required for Acceptance of a subsequent deliverable, then Successful Respondent shall perform such modification or rework at no charge and each Party's obligations, rights, and remedies described herein shall continue to apply.

#### **10.10. Deliverables Credits**

Successful Respondent recognizes that DIR is paying Successful Respondent to provide certain Critical Deliverables by the time and in the manner agreed by the Parties. If Successful Respondent fails to meet its obligations with respect to such Critical Deliverables, then, in addition to other remedies available to DIR, Successful Respondent shall pay or credit to DIR the amounts specified in Article [6 Performance Model and Service Level Agreements](#) as applicable, or established by DIR as part of the Project approval process on a case by case basis in recognition of the diminished value of the Services resulting from Successful Respondent's failure to meet the agreed upon level of performance, and not as a penalty (the "**Deliverable Credits**"). If DIR recovers monetary damages from Successful Respondent as a result of Successful Respondent's failure to meet its obligations with respect to one (1) or more Critical Deliverables, Successful Respondent shall be entitled to set-off against such damages any Deliverable Credits paid for the failures giving rise to such recovery. Deliverable Credits are distinct from Service Level Credits and shall not be counted toward or subject to the overall cap on Successful Respondent's liability.

## 11. Contract Conclusion Requirements: Transition to Successor at Contract Termination

### 11.1. Overview

- (a) Successful Respondent will provide to DIR the Termination Assistance Services set forth herein in connection with the termination or expiration of the Contract.
- (b) To the extent the Termination Assistance Services include any tasks which Successful Respondent is not otherwise obligated to perform under the Contract, the charges will be based on then-current rates for Services as proposed by Successful Respondent in this Exhibit or prevailing rates at the time of termination, whichever is lower.
- (c) “Termination Assistance Services” will mean:
  - (i) to the extent requested by DIR, the continued performance by Successful Respondent of its obligations under the Contract (including providing the Services which are subject to termination or expiration), and
  - (ii) the provisioning of such assistance, cooperation and information as is necessary to help enable a smooth transition of the applicable Services to DIR or its designated third-party provider (“Successor”).
- (d) As part of Termination Assistance Services, the Successful Respondent will provide such information as DIR may request relating to the number and function of each of the Successful Respondent personnel performing the Services, and Successful Respondent will make such information available to the Successor designated by DIR.
- (e) The Successful Respondent will cooperate with DIR in its attempts at transferring the services responsibilities to another provider in a manner in keeping with not adversely affect the provision of ongoing services.

### 11.2. Termination Assistance Services

#### 11.2.1. General

Upon DIR's request, Successful Respondent shall provide Termination Assistance Services directly to DIR, any DCS Customer, any successors or assignees of such Entities and any of their designee(s).

##### 11.2.1.1. Period of Provision

Successful Respondent shall provide Termination Assistance Services commencing on the date a determination is made by DIR that there shall be an Assistance Event, which date may be up to twenty-four (24) months prior to effective date of such Assistance Event or on such earlier date as DIR may request, and continuing for up to three (3) months after the effective date of such Assistance Event, as designated by DIR, subject to such further extensions as permitted in **MSA Section 4.2 Use of Third Parties**.

##### 11.2.1.2. Notice of an Assistance Event

DIR will provide Successful Respondent with written notice of an Assistance Event. Such notice will include a description of the Services that are to be terminated or discontinued, the affected DCS Customers, and the anticipated effective date of the Assistance Event. DIR may modify or update any of the information provided in the initial notice of an Assistance Event from time to time by a supplemental notice from DIR to Successful Respondent.

#### 11.2.1.3. Extension of Termination Assistance Services

DIR may elect to end the period for performance of Termination Assistance Services (in whole or in part), in its sole discretion, and restart the period for performance of Termination Assistance Services provided that the total of all such delays shall not result in Termination Assistance Services being performed for no more than a total of twenty-seven (27) months without Successful Respondent's consent.

#### 11.2.1.4. Firm Commitment

Successful Respondent shall provide Termination Assistance Services regardless of the reason for the Assistance Event (including a termination for cause by Successful Respondent). Successful Respondent shall maintain capability on at least thirty (30) days notice at all times during the Term to deploy all necessary resources to perform any Termination Assistance Services.

#### 11.2.1.5. Performance

Successful Respondent shall provide all Termination Assistance Services subject to and in accordance with the terms and conditions of this Agreement. Successful Respondent shall perform Termination Assistance Services with at least the same degree of accuracy, quality, completeness, timeliness, responsiveness and resource efficiency as it is or was required to provide the same or similar Services in accordance with this Agreement. The quality and level of performance of Termination Assistance Services provided by Successful Respondent shall continue to meet or exceed the Service Levels and shall not be degraded or deficient in any respect. Service Level Credits shall be assessed for any failure to meet Service Levels during any period in which Termination Assistance Services are provided. If any period for performing any Termination Assistance Services extends beyond the expiration or the effective date of any termination of this Agreement, the provisions of this Agreement shall remain in full effect for the duration of such period.

#### 11.2.2. Scope

As part of the Termination Assistance Services, Successful Respondent shall timely transfer the control and responsibility for Services previously performed by or for Successful Respondent to DIR, the DCS Customers and/or their designee(s), and upon DIR request, shall execute any documents reasonably necessary to affect such transfers. Successful Respondent shall also provide any and all information and assistance requested by DIR required for:

- (i) the Systems and processes associated with the Services to operate and be maintained and enhanced efficiently;
- (ii) the Services to continue without interruption or adverse effect; and

**State of Texas** Department of Information Resources, Data Center Services

- (iii) the orderly transfer of the Services (or replacement or supplemental services) to DIR, the DCS Customers and/or their designee(s).

### 11.2.3. General Support

- (a) Prior to the Termination Assistance event, Successful Respondent shall:
  - (i) assist DIR, the DCS Customers, and/or their designee(s) in developing a written plan for the migration of the Services to DIR, the DCS Customers and/or their designee(s), which plan shall include (as requested by DIR) capacity planning, process planning, facilities planning, human resources planning, technology planning, telecommunications planning and other planning necessary to effect the transition,
  - (ii) perform programming and consulting services as requested to assist solely in implementing the transition plan,
  - (iii) train personnel designated by DIR, the DCS Customers and/or their designee(s) in the use of any processes or associated Equipment, Materials, Systems or tools used in connection with the provision of the Services as needed for such personnel to assume responsibility for performance of the Services,
  - (iv) provide a catalog of all processes, Materials, DIR Data, Equipment, Third Party Contracts, automation scripts, and tools used to provide the Services,
  - (v) provide machine readable and printed listings and associated documentation for source code for Software owned by DIR or any DCS Customer and source code to which DIR and/or the DCS Customers are entitled under this Agreement and assist in its re-configuration,
  - (vi) provide technical documentation for Software used by Successful Respondent to provide the Services as needed for continuing performance of the Services,
  - (vii) analyze and report on the space required for the DIR Data and the Software needed to provide the Services,
  - (viii) assist in the execution of data migration and testing process until the successful completion of the transition to DIR, the DCS Customers and/or their designee(s),
  - (ix) create and provide copies of the DIR Data in the format and on the media requested by DIR, the DCS Customers and/or their designee(s),
  - (x) provide a complete and up-to-date, electronic copy of the Service Management Manual (SMM) in the format and on the media requested by DIR, the DCS Customers and/or their designee(s), and
  - (xi) provide other technical and process assistance, documentation and information as requested by DIR, the DCS Customers and/or their designee(s).
- (b) After the Assistance Event and during the Termination Assistance Period, Successful Respondent shall answer any questions that may arise concerning the Services previously performed by the Successful Respondent. DIR may request Successful Respondent to provide certain discontinued Services after the Assistance Event; however, such Termination Assistance Services may include a charge as described in Section [11.2.13 Rates and Charges](#).

#### 11.2.4. Certain Materials

Successful Respondent shall provide source code and artifacts (e.g., documentation, use cases, test scripts, design models, activity diagrams and systems configuration) which Successful Respondent has in its possession, or Successful Respondent Agents have in their possession, for:

- (i) any modification or enhancement made hereunder by Successful Respondent to DIR Software,
- (ii) any Software developed pursuant to this Agreement which DIR owns or with respect to which DIR is otherwise entitled to source code, and
- (iii) as otherwise provided in an applicable Statement of Work;

#### 11.2.5. Right to Acquire

DIR, the DCS Customers and/or their designee(s) shall have the right (but not the obligation) to purchase any or all Software as a Service (SaaS) type systems and on-premise software licenses that are owned by Successful Respondent and implicated by the relevant Assistance Event subject to the requirements set forth in **MSA**.

#### 11.2.6. Personnel

##### 11.2.6.1. List of Successful Respondent Personnel

Successful Respondent shall promptly provide to DIR a list, organized by location, of the Successful Respondent Personnel assigned to the performance of the Services that are implicated by each Assistance Event. Such list shall, subject to applicable Privacy Laws, specify each such Successful Respondent Personnel's name, job title, compensation package, leave status, years of service and job responsibilities. DIR agrees not to disseminate the personally identifiable information contained in such list without Successful Respondent's consent. Successful Respondent shall not terminate, reassign or otherwise remove from the performance of the Services any such dedicated Successful Respondent Personnel until after the end of the applicable Termination Assistance Services period.

##### 11.2.6.2. Right to Hire

- (a) DIR, the DCS Customers, and/or their designee(s) shall be permitted, without interference (including through counter-offers) from Successful Respondent (subject to this Section), to meet with, solicit and hire, effective after the later of:
  - (i) the date of DIR's notice of an Assistance Event, and
  - (ii) the completion of the Termination Assistance Services requiring such Successful Respondent Personnel, any Successful Respondent Personnel substantially dedicated to the performance of the Services during the twelve (12) month period prior to the date of DIR's notice of an Assistance Event who are implicated by that Assistance Event.
- (b) Successful Respondent hereby waives its rights, if any, under contracts with such Successful Respondent Personnel restricting the ability of such Successful Respondent Personnel to be recruited or hired by DIR, the DCS Customers and/or their designee(s) (including waiving any right to restrict such personnel via non-compete agreements or other contractual means). Successful Respondent shall provide DIR, the DCS

Customers and/or their designee(s) with reasonable assistance in their efforts to meet with, solicit and hire such Successful Respondent Personnel, and shall give DIR, the DCS Customers and/or their designee(s) reasonable access to such Successful Respondent Personnel for interviews, evaluations and recruitment. DIR shall endeavor, and shall cause the DCS Customers and their designee(s) to endeavor, to conduct the above-described activities in a manner that is not unnecessarily disruptive of Successful Respondent's performance of its obligations under this Agreement.

#### 11.2.6.3. Subcontractor Employees

- (a) With respect to Subcontractors, Successful Respondent shall:
  - (i) obtain for DIR, the DCS Customers and their designee(s) the rights specified in Section [11.2.6.2 Right to Hire](#), and
  - (ii) ensure that such rights are not subject to subsequent Subcontractor approval or the payment of any fees, charges or other amounts.
- (b) If Successful Respondent is unable to obtain any such rights with respect to a Subcontractor, it shall notify DIR in advance and Successful Respondent shall not subcontract any Services to such Subcontractor without DIR's prior approval (and absent such approval, Successful Respondent's use of any such Subcontractor shall obligate Successful Respondent to obtain or arrange, at no additional cost to DIR, the rights specified in Section [11.2.6.2 Right to Hire](#), for DIR, the DCS Customers and their designee(s)).

#### 11.2.7. Intentionally Left Blank

#### 11.2.8. Equipment

##### 11.2.8.1. List of Equipment

Successful Respondent shall promptly provide to DIR a list, organized by location, of the Equipment that is implicated by each Assistance Event. Such list shall specify information requested by DIR, including all fields tracked by Successful Respondent in any asset management system used by Successful Respondent for tracking and managing Equipment, such Equipment's function, manufacturer, model number, age, and other pertinent information.

##### 11.2.8.2. Right to Acquire

DIR, the DCS Customers and/or their designee(s) shall have the right (but not the obligation) to purchase or (subject to Section 11.2.10 DIR Facilities, Equipment, and Materials) assume the lease for any or all Equipment that is owned or leased by Successful Respondent and that is implicated by the relevant Assistance Event. Subject to Section 11.2.10 DIR Facilities, Equipment, and Materials, such Equipment shall be transferred in good working condition, reasonable wear and tear excepted, as of the later of the effective date of the relevant Assistance Event and the completion of the Termination Assistance Services requiring such Equipment. Successful Respondent shall maintain such Equipment through the date of transfer so as to be eligible for the applicable manufacturer's maintenance program. In the case of Successful Respondent-owned Equipment (including Equipment owned by Successful Respondent Affiliates and Subcontractors and further including any such Equipment leased to **State of Texas** Department of Information Resources, Data Center Services

Successful Respondent), Successful Respondent (or such Affiliate or Subcontractor) shall grant to DIR, the DCS Customers, and/or their designee(s) a warranty of title and a warranty that such Equipment is free and clear of all liens, security interests, and other encumbrances. Such conveyance by Successful Respondent (or Affiliate or Subcontractor) to DIR, the DCS Customers, and/or their designee(s) shall be at fair market value (as shall be determined by an agreed-upon appraisal); provided, however, in the case of any item of Equipment for which the acquisition cost has been the basis of Charges to DIR (e.g., as in the case of the Hardware Service Charge provided in **Exhibit 2 Pricing**), such conveyance shall be at an amount not exceeding the amount of any then unrecovered acquisition cost computed in accordance with the method used to charge DIR therefor. At DIR's request, the Parties shall negotiate in good faith and agree upon the form and structure of the purchase. In the case of leased Equipment, Successful Respondent shall:

- (i) represent and warrant that the lease is not in default,
- (ii) represent and warrant that all payments thereunder have been made through the date of transfer, and
- (iii) notify DIR, the DCS Customers, and/or their designee(s) of any lessor defaults of which it is aware at the time.

#### 11.2.9. Lease of Data Center

Successful Respondent shall arrange that the owner or leaseholder of the DIR Consolidated Data Center lease such facility(s) to DIR, the DCS Customers and/or their designee(s) on commercially reasonable terms and conditions and providing at a minimum a level of access and use of such facility(s) reasonably necessary to continue the provision from such facility(s) of the Services that were performed from such facility(s) during the Term. In no event shall the term of such lease be required to exceed the term of the leaseholder's lease. Upon the occurrence of the event described in Section [11.2.15 Information](#) or DIR's notice of an Assistance Event, Successful Respondent will provide to DIR, or its designee, copies of all leases and related information, including, without limitation, base rent, deposit, and all related financial information.

#### 11.2.10. DIR Facilities, Equipment, and Materials

Successful Respondent shall vacate the DIR Facilities and return to DIR, if not previously returned, any resources that are implicated by the relevant Assistance Event and that are owned, leased or licensed by DIR, any DCS Customer, or any DIR Contractor, including DIR owned or leased Equipment, DIR Owned Materials and DIR licensed Materials, in condition at least as good as the condition of such facilities and resources when they were made available to Successful Respondent, ordinary wear and tear excepted. Such facilities and resources shall be vacated and/or returned as of the later of the effective date of the relevant Assistance Event and the completion of the Termination Assistance Services requiring such facilities or resources.

#### 11.2.11. Third Party Contracts

Successful Respondent shall promptly, but no less than thirty (30) days from DIR's issuance of notice of an Assistance Event, provide to DIR a list of the Third Party Contracts that are implicated by the relevant Assistance Event. At any time during the contract term, DIR may request and Successful Respondent shall provide the Third **State of Texas** Department of Information Resources, Data Center Services

Party Contract(s) in accordance with **MSA, Section 4.16.3**, regardless of whether Successful Respondent's other customers utilize or benefit from such Third Party Contract(s), allowing DIR to disclose such contracts during future procurements. Except for the Third Party Contracts specified in **Exhibit 2 Pricing**, in accordance with MSA, Section 4.16.3 subject to Section 11.2.10 DIR Facilities, Equipment, and Materials, Successful Respondent shall, at DIR's request, cause the counter-parties to such Third Party Contracts to permit DIR, the DCS Customers, and/or their designee(s) to assume prospectively any or all such Third Party Contracts or to enter into new contracts with DIR, the DCS Customers, and/or their designees on substantially the same terms and conditions, including price. Successful Respondent shall transfer or assign those Third Party Contracts that DIR elects to assume prospectively to DIR, the DCS Customers, and/or their designee(s) as of the later of the effective date of the relevant Assistance Event and the completion of the Termination Assistance Services requiring such Third Party Contracts. Such transfers or assignments shall be on terms and conditions acceptable to all applicable parties, provided that:

- (i) there shall be no fee, charge or other amount imposed on DIR, the DCS Customers, and/or their designee(s) by Successful Respondent or the counter-parties to such Third Party Contracts for such transfer or assignment, and
- (ii) Successful Respondent shall:
  - A. promptly cure and, in accordance with **MSA Section 10.1.3 Licenses, Leases, and Contracts**, indemnify DIR against any default under such Third Party Contracts relating to the period prior to such transfer or assignment;
  - B. represent and warrant that all payments thereunder through the date of transfer or assignment are current; and
  - C. notify DIR, the DCS Customers, and/or their designee(s) of any counter-party's default with respect to such Third Party Contracts of which it is aware at the time of such transfer or assignment.

#### 11.2.12. Other Subcontracts and Third Party Contracts

With respect to Third Party Contracts implicated by the relevant Assistance Event that are not otherwise transferred or assigned to DIR, the DCS Customers, and/or their designee(s) pursuant to **MSA Section 4.2.2 Successful Respondent Cooperation**, Successful Respondent shall make available to DIR, the DCS Customers, and/or their designee(s), pursuant to reasonable terms and conditions, any Third Party services then being utilized by Successful Respondent in the performance of the Services. Successful Respondent shall retain the right to utilize any such Third Party services in connection with the performance of services for other Successful Respondent customers. DIR and the DCS Customers shall retain the right to contract directly with any third party previously utilized by Successful Respondent to perform any Services.

#### 11.2.13. Rates and Charges

- (a) Except as provided in this Subsection and **MSA Section 4.2.2 Successful Respondent Cooperation**, Successful Respondent shall provide all Termination Assistance Services at no additional charge. The Parties anticipate that Termination Assistance Services requested by DIR shall be provided by Successful Respondent using Successful Respondent Personnel already assigned to the performance of the Services and **State of Texas** Department of Information Resources, Data Center Services

without adversely affecting Successful Respondent's ability to meet its performance obligations. To the extent DIR requests that Successful Respondent perform only a portion (but not all) of the Services included in a particular Charge, the amount to be paid by DIR shall be equitably adjusted downward in accordance with **Exhibit 2 Pricing**, to the extent applicable, or equitably adjusted downward in proportion to the portion of the Services that Successful Respondent shall not be providing to the extent that **Exhibit 2 Pricing** does not provide for such reduction. If and to the extent Termination Assistance Services requested by DIR cannot be provided by Successful Respondent using Successful Respondent Personnel then-assigned to the performance of the Services without adversely affecting Successful Respondent's ability to meet its performance obligations, DIR, in its sole discretion, may:

- (i) forego or delay any work activities or temporarily or permanently adjust the work to be performed by Successful Respondent, the schedules associated therewith or the Service Levels to permit the performance of such Termination Assistance Services using such personnel, or
  - (ii) authorize Successful Respondent to use additional Successful Respondent Personnel to perform Termination Assistance Services.
- (b) To the extent DIR authorizes Successful Respondent to use additional Successful Respondent Personnel to perform Termination Assistance Services requested by DIR, DIR shall pay Successful Respondent the applicable rates and charges specified in **Exhibit 2 Pricing** for such Full-time Positions (FTPs) or Full-time Equivalent (FTEs) or, if no such rates and fees are specified in **Exhibit 2 Pricing**, a negotiated fee for the additional Successful Respondent Personnel required to perform such Termination Assistance Services (determined on the basis of pricing no less favorable to DIR than the pricing and labor rates set forth herein for comparable Services), provided that Successful Respondent notifies DIR in advance of any such charges, obtains DIR's approval prior to incurring such charges, and uses commercially reasonable efforts to minimize such charges. Notwithstanding the foregoing, DIR will not be obligated to pay Successful Respondent for any such additional Successful Respondent Personnel if at any time prior to DIR's issuance of the notice of Assistance Event, Successful Respondent failed to sufficiently staff the Services that are the subject of the Assistance Event (both with respect to number of personnel and personnel with the necessary skills and training).

#### 11.2.14. Proprietary Communications Network

If Successful Respondent uses a proprietary communications network to provide the Services, then for a period of up to two (2) years following the effective date of the relevant Assistance Event, Successful Respondent shall, if requested by DIR, continue to provide such proprietary communications network and other network Services to DIR, the DCS Customers, and/or their designee at the rates, and subject to the terms and conditions, set forth in this Agreement.

#### 11.2.15. Information

Upon the occurrence of any breach by Successful Respondent under this Agreement or if DIR elects to evaluate re-procurement of all or any portion of the Services, Successful Respondent will provide to and/or make available for DIR review any and all reports, data and information that DIR deems necessary in order to evaluate all options

**State of Texas** Department of Information Resources, Data Center Services

related to such breach and/or re-procurement, including without limitation, all reports, data and information specified in **MSA Section 4.2.1 Right of Use**. For the avoidance of doubt, Successful Respondent will be obligated to provide all such reports, data and information regardless of whether DIR has provided notice of or otherwise declared an Assistance Event.

### **11.3. Successful Respondent Sourced and Managed Contracts**

- (a) The Successful Respondent shall ensure that all Successful Respondent-sourced contracts inclusive of general building maintenance and repairs, telecommunications, environmental testing, facility mechanical maintenance (e.g., UPS and diesel/fuel power generation) that do not support DCS Customer operations are terminated (save for those contracts that DIR assumes or those that DIR requires the Successful Respondent assign or transfer to DIR or its designee), and that DIR is not obligated to any ongoing financial, contractual or other obligations associated with these contracts or any Successful Respondent or third-party services, equipment or maintenance that support these contracts.
- (b) The Successful Respondent shall transfer the terminated or expired Services to DIR or its designee(s)/successor(s) in an efficient and orderly manner.
- (c) Prior to such actions being taken, the Successful Respondent shall verify with DIR that the impact on DIR's business (including its personnel and customers) and the internal and third-party IT-related costs incurred by DIR in transferring the terminated services are acceptable to DIR under the circumstances.
- (d) The Successful Respondent shall continue to perform such services without disruption or deterioration until the transfer has occurred:
  - (i) consistent with the terms and conditions of this Contract, or
  - (ii) except as approved by DIR.
- (e) In an effort to facilitate transition of responsibilities, the Key Management Position obligations in [Section 5.7 Evergreen Service Personnel](#) will continue to apply during the agreed Termination Assistance Period.

### **11.4. Termination Assistance Plan**

The contents of Termination Assistance Plan will include, unless otherwise agreed, the services, functions, and activities as defined below:

- (i) Documentation of existing and planned Projects and support activities;
- (ii) Identification of the Services and related positions or functions that require transition and a schedule, plan and procedures for DIR or its designee assuming or reassuming responsibility;
- (iii) Description of actions to be taken by the Successful Respondent in performing termination assistance;
- (iv) Description of how the transfer of:
  - A. relevant information regarding the Services,
  - B. resources (if any),
  - C. operations, and
  - D. contracts (if any) will be achieved;

- (v) Description in detail of any dependencies on the successors necessary for the Successful Respondent to perform the termination assistance services (including an estimate of the specific Successful Respondent staffing required);
- (vi) Inventory of documentation and work products required to facilitate the transition of responsibilities;
- (vii) Assist DIR in the identification of significant potential risk factors relating to the transition and in designing plans and contingencies to help mitigate the risk;
- (viii) Set out the timeline for the transfer of each component of the terminated Services (including key milestones to track the progress of the transfer); and
- (ix) Define a schedule and plan for the Successful Respondent's return to DIR of:
  - A. the Service locations then occupied by the Successful Respondent (if any), and
  - B. DIR or DCS Customer confidential information, DIR or DCS Customer data, documents, records, files, tapes and disks in the Successful Respondent's possession.

### **11.5. Termination Management Team**

- (a) The Successful Respondent will provide a senior Project manager who will be responsible for the Successful Respondent's overall performance of the termination assistance services and who will be the primary point of contact for DIR in respect of the termination assistance services during the termination assistance period.
- (b) DIR will appoint a senior Project manager who will be the primary point of contact for the Successful Respondent during the termination assistance period. Additionally, DIR may appoint a transformation team that would be responsible for the review of then current services provided by the Successful Respondent and work to facilitate an orderly transition of services.

### **11.6. Operational Transfer**

- (a) The Successful Respondent will perform the following activities to help effect a smooth and orderly transfer of operational responsibility for the terminated services:
  - (i) Facilitating access to DIR source code, object code, object and production libraries, reference files, field descriptions, record layouts and technical specifications along with run documentation for DIR software then in the Successful Respondent's possession including: tools, scripts, run books, production schedules and procedures as required to support the in-scope applications which may be used in training, knowledge transfer, sizing assessments, operational reviews and other uses required by DIR at the time of transfer.
  - (ii) Cooperate with the Successors in conducting migration testing.
  - (iii) Providing DIR-owned documents and information related to the functionality, program code, data model and data base structure, and access methods for the in-scope applications and manual and automated processes used for DIR, within the possession or control of the Successful Respondent, and reviewing such processes, documents and information with the Successor as requested.
  - (iv) Cooperate with DIR's test plans, back out procedures, and contingency plans as part of the migration of terminated services.
- (b) After the transfer of the provision of terminated services to DIR, its designee(s), or both, providing additional assistance as requested by DIR to facilitate continuity of operations, through the end of the termination assistance period.

## 12. Other Requirements

### 12.1. Support Requirements

- (a) The Respondent must describe the support it wants from DIR other than what DIR has offered in this Exhibit. Specifically, the Respondent must address the following:
- (i) Nature and extent of DIR support required in terms of staff roles, percentage of time available, etc.;
  - (ii) Assistance from DIR staff and the experience and qualification levels required; and
  - (iii) Other support requirements.
- (b) DIR may not be able or willing to provide the additional support the Respondent lists in this part of its Proposal. The Respondent therefore must indicate whether its request for additional support is a requirement for its performance. If any part of the list is a requirement, DIR may reject the Respondent's Proposal, if DIR is unable or unwilling to meet the requirements.

### 12.2. Materials

Successful Respondent shall not utilize any Successful Respondent Owned Materials that are not commercially available.

<End of Statement of Work>