

**State of Texas**  
**Department of Information Resources**



**Attachment 1.3**  
**Version 2.1**

**Service Level Definitions and Performance Analytics**

**DCS Security Operations Services**  
**DIR-SECOPS-MSA-434**

## Table of Contents

<b>1. CRITICAL SERVICE LEVELS</b>	<b>4</b>
1.1. Resolution Time (Severity 1 - 4)	4
1.2. Time to Initiate Security Incident Response Team (SIRT) Bridge	5
1.3. Service Availability	5
1.4. Chronic Incidents: Root Cause Analysis, Corrective Actions and Recidivist Rate	6
1.5. Service Request Fulfillment Timeliness	6
1.6. Solution Implementation Time	7
1.7. Solution Proposal Delivery Timeliness	7
<b>2. KEY SERVICE LEVELS</b>	<b>8</b>
2.1. Data Quality	8
2.2. Security Incident Communication	9
2.3. Security Event Identification – Time To Respond	10
2.4. Timely Security Vulnerability Disposition	11
2.5. Change Management Effectiveness	12
2.6. License and Maintenance Renewal Timeliness	12
2.7. Invoice Dispute Resolution	13
2.8. Patch Compliance	14
<b>3. KEY PERFORMANCE INDICATORS</b>	<b>15</b>
3.1. Shared Services Growth	15
3.2. Customer Satisfaction	17
3.3. Service Quality	18
3.4. Value	19
3.5. Security	21
<b>4. OPERATING MEASUREMENTS</b>	<b>22</b>
4.1. Percentage of change in number of Major Incidents	22
4.2. Percentage of Customers satisfied with service offerings	22
4.3. Problem: Time to Review and Deliver RCA	22
4.4. Asset: Assets Updated by eDiscovery	23
4.5. Asset: Asset Attributes Updated Electronically	23
4.6. Invoicing: Invoice Delivered On-time	23
4.7. Invoicing: Time to Assign Invoice Dispute	23
4.8. Devices Reporting via Electronic Management Tool	23
4.9. Growth in Number of Customers	23
4.10. Growth in Shared Services Volume	23
4.11. Growth in Number of Services Offered	24
4.12. Growth in Shared Services Spend per Customer	24
4.13. Growth in Shared Services Spend by Customers other than State Agencies	24
4.14. Percentage of Executive/IT Operational Staff Customers Satisfied	24
4.15. Monthly Customer Scorecard – <b>Acceptable</b>	24
4.16. Customer Service Desk Survey	24
4.17. <INTENTIONALLY LEFT BLANK>	24
4.18. <INTENTIONALLY LEFT BLANK>	24
4.19. Percentage of Service Levels Meeting Expected <b>Targets</b>	25
4.20. Service Request Fulfillment <b>in Days</b>	25
4.21. Percentage of Automated Processes	25
4.22. Percentage of Software at N-2 or Higher	25
4.23. Percentage of Software that is Supported	25
4.24. Percentage of Hardware Less Than <b>5 Years Old</b>	25
4.25. Percentage of Spend within Market Range	25
4.26. Percentage of Service Requests Self-Provisioned Through Service Catalog	25
4.27. Change in Risk Based on Vulnerability Scan Measures	26
4.28. Change in Annual Common Security Framework (CSF) Maturity Rating	26
4.29. Percentage of Security Devices monitored by Security Incident and Event Management (SIEM)/Security Analytical Devices	26
4.30. Percentage Change in Number of Major Security Incidents	26
<b>5. OPERATIONAL REPORTS</b>	<b>26</b>



## 1 Critical Service Levels

This Section sets forth qualitative descriptions of the Critical Service Levels. The numerical Minimum Service Levels and commencement of obligations associated with such Critical Service Levels are set forth in **Attachment 1.2 Service Level Matrix**.

### 1.1 Resolution Time (Severity 1 - 4)

<b>Business Intent:</b>	Prompt resolution of Service incidents and outages that impact DIR Customer processing and processes
<b>Type:</b>	R
<b>Applicable Service Component(s)</b>	Security Operations Services, MSI, TBD
<b>Definition:</b>	<p>Resolution Time measures the percentage of time the Successful Respondent resolves Severity Level 1 - 4 Incidents within the applicable timeframes in the table below.</p> <p>Incident Resolution (Severity 1 - 4) will be determined by determining the elapsed time (stated in hours and minutes) representing the statistical mean for all Severity 1 - 4 Incidents for in-scope Services in the Measurement Window. Resolution Time” is measured from time that the Incident is received at the MSI Service Desk to the point in time when the incident is resolved, or workaround is in place.</p> <p>Severity 1 - 4 incidents will be categorized in the SMM. All emergency offboarding notices will be entered as Severity 1 incidents.</p> <p>The Successful Respondent will report updates and progress to DIR as defined in the SMM for this SLA. The Service Level calculation is the total number of Severity 1 - 4 Incidents for which the Resolution Time is less or equal to the relevant resolution timeframe, divided by the total number of Resolved Incidents plus the total number of open Incidents that have exceeded the relevant resolution timeframe, with the result expressed as a percentage.</p> <p>For purposes of clarity, note the following:</p> <p>(a) if an Incident is opened within the current Measurement Window, but its relevant resolution timeframe extends beyond the end of the current Measurement Window, then it is excluded from the current Measurement Window’s calculation (unless such Incident is actually Resolved in the current Measurement Window, in which case it is included in the current Measurement Window’s calculation)</p> <p>(b) an open Incident that has exceeded the relevant resolution timeframe is also carried forward into subsequent Measurement Windows as a breach until Resolved; if it is resolved within twenty-eight (28) days following its relevant resolution timeframe, it is excluded from the subsequent measurement window; otherwise, it is counted as failed to meet the resolution timeframes in each subsequent Measurement Window’s calculation until Resolved.</p>
<b>Formula:</b>	$\text{Response Time} = \frac{\text{Total number of resolved Severity 1 - 4 Incidents that met resolution time target}}{\text{Total number of resolved Severity 1 - 4 Incidents plus open incidents that should have been resolved during the measurement window}}$
<b>Measurement Window:</b>	Reporting Month
<b>Data Source:</b>	<p>Incident tickets will be logged in the MSI ITSM system. Incidents will be categorized and assigned to resolver teams who will work to resolve the incident and progress the ticket through the incident management lifecycle.</p> <p>Incident data will be uploaded to ServiceFlow on a daily basis. ServiceFlow will filter incident tickets based on appropriate measurement criteria.</p>
<b>Frequency of Collection:</b>	Per incident

Table 1: Resolution Time Service Level Measures

Severity Level	Resolution Time
Severity 1	<= 2 hours
Severity 2	<= 3 hours
Severity 3	<= 3 business days
Severity 4	<= 7 business days

### 1.2 Time to Initiate Security Incident Response Team (SIRT) Bridge

<b>Business Intent:</b>	The intent of this metric is to ensure timely establishment of SIRT bridge to lead security incident triage across resolver groups and Customer stakeholders for effective collaboration timely resolution.	
<b>Type:</b>	U	
<b>Applicable Service Component(s)</b>	Security Operations Services	
<b>Definition:</b>	The Service Level for “Time to Initiate SIRT Bridge” measures the percentage of time the Successful Respondent initiates a SIRT bridge with the required resolver and Customer teams and by commencing the bridge within fifteen (15) minutes of declaration of a SIRT. Trigger events that are used to declare a SIRT will be maintained in the SMM.	
<b>Formula:</b>	Time to Initiate SIRT	$\frac{\text{Total number of SIRTs initiated within 15 minutes of SIRT declaration}}{\text{Total number of SIRTs initiated}}$
<b>Measurement Window:</b>	Monthly	
<b>Data Source:</b>	ServiceNow	
<b>Frequency of Collection:</b>	Real time	

### 1.3 Service Availability

<b>Business Intent:</b>	The Service is available to Customers, MSI, and applicable SCPs and performing within expected norms. Systems and Services are responsive and productive work can be performed without delays to business process or applications.	
<b>Type:</b>	U	
<b>Applicable Service Component(s)</b>	Security Operations Services	
<b>Definition:</b>	<p>This SLA measures the percentage of time Security Systems and Services are Available to the end-user during the applicable Measurement Window.</p> <p>If Downtime occurs for Security System or Service, the Outage is counted against the Configuration Item (CI), and the affected System or Service is considered unavailable for purposes of this Service Level. Downtime begins upon the Start Time of the Outage. If a Security System or Service is supported by multiple CIs, then only the CIs associated with the Downtime are considered unavailable.</p> <p>If an Infrastructure Instance itself appears to be operational, but the System or Service running on the infrastructure is not Available, then the Infrastructure Instance is considered unavailable.</p> <p>Scheduled hours of operations and maintenance windows for each infrastructure element related to the Security Systems and Services will be maintained in the SMM. Scheduled maintenance time is not counted against this Availability SLA.</p>	
<b>Formula:</b>	Service Availability and Responsiveness	$\frac{\text{Total actual Availability for each of the Monitored Infrastructure Elements}}{\text{Total Availability time for each element less planned maintenance}}$
<b>Measurement Window:</b>	Monthly	
<b>Data Source:</b>	Infrastructure Monitoring Tools.	
<b>Frequency of Collection:</b>	Real time	

1.4 Chronic Incidents: Root Cause Analysis, Corrective Actions and Recidivist Rate

**Business Intent:** Incidents affecting Service and security operations and monitoring, online batch or otherwise, are promptly addressed, prioritized and resolved to the satisfaction of DIR or DIR Customers and do not reoccur or cause corollary issues to occur as a result of the repair to the element that was the root cause of the Incident.

**Type:** R

**Applicable Service Component(s)** Security Operations Services, MSI, TBD

**Definition:** This SLA measures the number of times the same Configuration Item experiences an Incident due to the same circumstance, reason or cause.

Once a Root Cause Analysis (RCA) is triggered for an incident, the incident is then qualified for inclusion in this SLA measurement. Recurring incidents will be counted against this SLA regardless whether the RCA is completed yet or whether the corrective actions have been completed yet. The intent of the SLA is to incentivize prompt and accurate root cause analysis and associated corrective actions.

**Formula:**

$$\text{Chronic Incidents} = \frac{(\text{Total number of RCAs initiated within the current and 2 prior measurement windows}) - (\text{Number of RCAs that had an additional incident due to the same circumstance, reason, or cause})}{(\text{Total number of RCA's initiated from rolling 3 months})}$$

**Measurement Window:** Monthly

**Data Source:** Information Technology Service Management (ITSM) system

**Frequency of Collection:** Monthly

1.5 Service Request Fulfillment Timeliness

**Business Intent:** Ensure all service requests are performed based upon turnaround times documented in the SMM as to result in predictable operational change cycles for DCS SCPs, MSI and Customers.

**Type:** R

**Applicable Service Component(s)** Security Operations Services, MSI, TBD

**Definition:** The Service Level for “Service Request Fulfillment” measures the percentage of time Successful Respondent successfully completes “Service Requests” (which are defined as requests that are not automated self-provisioned or that do not require solution proposal development).

Specific target timeframes are maintained in the SMM.

**NOTE:** The current Service Request target timeframes are documented in the SMM. DIR expects the Respondent to propose improvements to the target timeframes based on its solution, automation, and workflow orchestration.

**Formula:**

$$\text{Service Request Fulfillment Timeliness} = \frac{\text{Total Number of Service Requests Performed within SMM Defined Turnaround Times}}{\text{Total Number Service Requests}}$$

**Measurement Window:** Month

**Data Source:** IT Service Management system

**Frequency of Collection:** Daily

1.6 Solution Implementation Time

**Business Intent:** Solutions are delivered to Customers in keeping with the commitments made in Solution Proposals at the agreed upon quality levels.

**Type:** R

**Applicable Service Component(s)** Security Operations Services, MSI, TBD

**Definition:** The Service Level for “Solution Implementation Time” measures the percentage of time Successful Respondent successfully implements a Solution Request within the committed timeframe. All phases of the Solution implementation process from DIR Customer approval of the solution proposal through successful implementation (which requires DCS Customer acceptance) into production are included in this measure.

The committed timeframe is that timeframe specified in the proposal (as further described in the “Solution Proposal Delivery” Service Level) or otherwise as agreed by the requester.

The Service Level calculation for “Solution Implementation” is the total number of projects that are successfully implemented within the committed timeframes, divided by the total number of projects implemented plus the total number of projects that have passed the committed timeframe, with the result expressed as a percentage.

Projects will be reported in the Measurement Window in which the associated Change ticket is closed, allowing sufficient time to determine if the project was successful.

For purposes of clarity, note the following:

1. if a project is assigned within the current Measurement Window, but its relevant committed timeframe extends beyond the end of the current Measurement Window, then it is excluded from the current Measurement Window’s calculation (unless such project is actually implemented in the current Measurement Window, in which case it is included in the current Measurement Window’s calculation)
2. an uncompleted project is also carried forward into subsequent Measurement Windows as a breach until implemented; if it is resolved within twenty-eight (28) days following its relevant committed timeframe, it is excluded from the subsequent Measurement Window; otherwise, it is counted as failed to meet the committed timeframes in each subsequent Measurement Window’s calculation until implemented.

**Formula:**

$$\text{Solution Implementation Time} = \frac{\text{Total Number of Solutions Implemented within the Proposed Timeframe}}{\text{Total completed Solution Implementations plus open Solution Implementations that have passed committed timeframe}}$$

**Measurement Window:** Month

**Data Source:** MSI ITSM, Solution Request System

**Frequency of Collection:** Monthly

1.7 Solution Proposal Delivery Timeliness

**Business Intent:** The Service Level for “Solution Proposal Delivery Timeliness” measures the percentage of time Successful Respondent delivers viable proposals to DCS Customers within the committed timeframes, in response to a solution request. A viable proposal is defined as one that has all the required architecture and cost elements required to deliver a viable solution.

**Type:** R

**Applicable Service Component(s)** Security Operations Services, MSI, TBD

**Definition:** Requests are worked in the approved prioritization order of the DCS Customer. Following validation of requirements, the Successful Respondent shall deliver a proposal for each request within the process and timeframes defined in the SMM. The MSI will assign in the Solution Request a timeframe for the Successful Respondent to deliver the proposal.

When a proposal is delivered, it must include a committed timeframe for project implementation specified as Business Days. This committed number of Business Days will be used in the “Solution Implementation” Service Level.

Specific sizing criteria and guidelines shall be maintained in the SMM.

Each proposal submitted to DCS Customers will be counted as a measurable event. If there are multiple proposals for one request due to requirements changes then subsequent iterations will be counted as another event. Each will count as an event and an opportunity to succeed or fail.

The Service Level calculation for “Solution Proposal Delivery” is the total number of solution proposals that are delivered within the committed timeframes, divided by the total number of delivered proposals plus the total number of open proposals that have exceeded the committed timeframes, with the result expressed as a percentage.

For purposes of clarity, note the following: (a) if a solution proposal request is opened within the current Measurement Window, but its relevant committed timeframe extends beyond the end of the current Measurement Window, then it is excluded from the current Measurement Window’s calculation (unless such request is actually delivered in the current Measurement Window, in which case it is included in the current Measurement Window’s calculation) (b) an open solution proposal request that has exceeded the committed timeframe is also carried forward into subsequent Measurement Windows as a breach until delivered; if it is resolved within twenty-eight (28) days following its relevant committed timeframe, it is excluded from the subsequent Measurement Window; otherwise, it is counted as failed to meet the committed timeframes in each subsequent Measurement Window’s calculation until delivered.

**Formula:**

$$\text{Solution Proposal Turnaround Time} = \frac{\text{Total Number of Solution Proposals Delivered within Required Timeframe}}{\text{Total Solution Proposals}}$$

**Measurement Window:** Month

**Data Source:** MSI ITSM system, Solution Request System

**Frequency of Collection:** Daily

## 2 Key Service Levels

This Section sets forth qualitative descriptions of the Key Service Levels. The numerical Minimum Service Levels and commencement of obligations associated with such Key Service Levels are set forth in **Attachment 1.2 Service Level Matrix**.

### 2.1 Data Quality

**Business Intent:** Data Quality Metric is designed to measure data quality within the CMDB. Data standards are defined and CMDB records in-scope are to adhere to it. The goal is correctness and completeness in the CMDB.

**Type:** R

**Applicable Service Component(s)** Security Operations Services, MSI, TBD

**Definition:** The Data Quality measure includes the assessment of critical attributes for key Security Operations processes using agreed business rules.

1. “Critical attributes” mean the attributes associated with the Configuration Items the Successful Respondent is responsible for maintaining or as required to support Security policies, standards and operations, for which quality data is necessary to successfully operate security processes (e.g., monitored in SIEM identifier, operating system, operating system version), as defined in the SMM.
2. “Key processes” mean those processes that are foundational to the delivery of services (e.g., Major Incident Management, Security Incident Management, Vulnerability Management), as defined in the SMM.
3. “Business rules” mean the set of checks that will be performed to on an attribute to determine quality, as defined in the SMM.

Data quality business rules will be run against the selected critical attributes on a regular basis within the Measurement Window. Data quality output will be loaded into the Digital MSI Service Level Reporting system on a regular basis within the Measurement Window, where the Service Level result will be calculated and reported based on appropriate measurement criteria.

The Service Level for “Data Quality” measures the percentage of critical attributes for key processes that meet the data quality standard. The key processes associated critical attributes and business rules will be maintained in the SMM.

The Service Level calculation for “Data Quality” is the total number of critical attributes that meet data quality standards for the CIs measured during the applicable Measurement Window, divided by the total number of critical attributes for the CIs measured during the applicable Measurement Window, with the result expressed as a percentage

**Formula:**

$$\text{Data Quality} = \frac{\text{Total Number of Configuration Items by critical attribute} - \text{Total Number of Configuration Items by critical attribute not meeting data quality}}{\text{Total Number of Configuration Items in Scope by critical attribute}}$$

**Measurement Window:** Month

**Data Sources:** ServiceNow CMDB

**Frequency of Collection:** Monthly

## 2.2 Security Incident Communication

**Business Intent:** The Security Incident Communication metric is designed to ensure timely and accurate communications to Authorized users and key program stakeholders in the event of a Security Incident.

**Type:** U

**Applicable Service Component(s)** Security Operations Services

**Definition:** The Service Level for “Security Incident Communication” measures the percentage of time Successful Respondent provides the notices to the applicable Authorized Users within the following timeframes with respect to Severity 1 and Severity 2 Security Incidents and that are not Resolved in less than one (1) hour from the Start Time for such Incident.

1. First notice: Within one (1) hour of Incident ticket creation
2. Subsequent notices: after each bridge call, or per the minimum time required below for Severity 1 and Severity 2 Security Incidents

A “notice” is defined as

1. Verbal communication to Authorized User, and as documented in the ticket
2. Bridge call including Authorized User, and as documented in the ticket
3. Email to Authorized User, and as documented in the ticket

Such notices shall not be deemed to have been provided unless (a) the Authorized User that reported the Security Incident has been contacted by the Successful Respondent and such notice of status has been provided or (b) Successful Respondent has left a voice mail (or if not possible because the Authorized User does not have a voice mail box, sent an email or attempted some other reasonable means of communication) for the Authorized User.

Severity 1 security Incidents are required to have communications, at a minimum, once every twelve (12) hours.

Severity 2 security Incidents are required to have communications, at a minimum, once every twenty-four (24) hours.

**Formula:**

$$\text{Security Incident Communication} = \frac{\text{Total number of Severity 1 and 2 Security Incidents that are resolved during the applicable Measurement Window, that have actual Resolution Times of greater than one (1) hour and for which Successful Respondent provided the applicable Authorized User the required notice(s)}}{\text{Total number of Severity 1 and Severity 2 Security Incidents, that are resolved during the applicable Measurement Window and that have actual Resolution Times of greater than one (1) hour}}$$

**Measurement Window:** Monthly

**Data Sources:** Information Technology Service Management (ITSM) system

**Frequency of Collection:** Daily

### 2.3 Security Event Identification – Time to Respond

**Business Intent:** The objective is to ensure events are acted upon and security incidents reported within required time frame.

**Type:** U

**Applicable Service Component(s)** Security Operations Services

**Definition:** The Service Level for “Security Event Identification – Time to Respond” measures the percentage of time the Successful Respondent responds to SIEM events by acknowledging each event using automated rules or by manually reviewing, within one (1) hour.

Measurement is based on SIEM logs whereas:

1. Acknowledged = an event is acknowledged when it is tagged or updated as being reviewed and responded to either using automation-based rules or triggers, or manually by human review.
2. Event Start = time the event is first captured and logged in the SIEM.
3. Event End = time the event is explicitly acknowledged automation-based rules or triggers, or manually by human event review.

Events that are not acknowledged within one (1) hour and events that were not acknowledged at all are considered as missing the SLA target.

For purposes of clarity, note the following:

1. if a security event is opened within the current Measurement Window, but its relevant acknowledgement timeframe extends beyond the end of the current Measurement Window, then it is excluded from the current Measurement Window’s calculation (unless such security event is actually acknowledge in the current Measurement Window, in which case it is included in the current Measurement Window’s calculation)
2. an open security event that has exceeded the relevant acknowledgement timeframe is also carried forward into subsequent Measurement Windows as a breach until acknowledged.

**Formula:**

$$\text{Security Event Identification – Time To Respond} = \frac{\text{Total number of SIEM events acknowledged within one (1) hour during the applicable Measurement Window}}{\text{Total number of SIEM events during the applicable Measurement Window}}$$

**Measurement Window:** Monthly

**Data Sources:** Successful Respondent SIEM logs including those that have an ‘acknowledged’ status and those not acknowledge within the Measurement Window.

**Frequency of Collection:** Daily

## 2.4 Timely Security Vulnerability Disposition

**Business Intent:** Ensure all security vulnerabilities are dispositioned for action to the appropriate entity (e.g., MSI, SCP, Customer) that can remediate the risk or vulnerability based upon disposition times documented in the SMM.

**Type:** U

**Applicable Service Component(s)** Security Operations Services

**Definition:** The Service Level for “Timely Security Vulnerability Disposition” measures the percentage of time Successful Respondent successfully dispositions a security vulnerability within the committed disposition timeframe. Specific disposition timeframes are maintained in the SMM.

Vulnerability inputs may come from various sources including at a minimum: SCP and MSI vulnerability scan results, Annual 3rd party Assessment results, MSBC results, SCP Audit results.

**Formula:**

$$\text{Timely Security Vulnerability Disposition} = \frac{\text{Total Number of Security Vulnerability Service Request tickets dispositioned within SMM Defined Disposition Times}}{\text{Total Number of Security Vulnerability Service Requests tickets}}$$

**Measurement Window:** Monthly

For this SLA Service Request tickets will be logged in the MSI ITSM system. Service Requests will be categorized as security vulnerability tickets.

**Data Sources:**

Incident data will be uploaded to ServiceFlow on a daily basis. ServiceFlow will filter incident tickets based on appropriate measurement criteria.

**Frequency of Collection:** Per Service Request

## 2.5 Change Management Effectiveness

**Business Intent:**

All changes to DCS environments follow a disciplined process, are authorized by the Customer and documentation is updated at all times to ensure that the Service environment of DCS is up to date and documentation is current. Environment changes are tested/validated and move as a comprehensive change package as opposed to piecemeal elements that result in unintended consequences.

**Type:**

R

**Applicable Service Component(s)**

Security Operations Services, MSI, TBD

**Definition:**

Changes are not successfully implemented if they:

1. do not comply with the Change Management procedures (including the Change Control Process), the SMM and any associated project plan,
2. were not approved by the Customer,
3. cause either a Severity 1 Incident or Severity 2 Incident,
4. exceeded the change window,
5. are backed out, or
6. partial success of change is backed out or unsuccessful.

Any change to DCS environments that met one or more of the above criteria is considered unsuccessful.

**Formula:**

$$\text{Change Management Effectiveness} = \frac{\text{Total Number of Successful Changes}}{\text{Total Number of Changes}}$$

**Measurement Window:** Monthly

**Data Sources:** Information Technology Service Management (ITSM) system

**Frequency of Collection:** Each Change to DCS Environment

## 2.6 License and Maintenance Renewal Timeliness

**Business Intent:**

The Service Level for “License and Maintenance Renewal Timeliness” measures the timeliness of all software license and hardware maintenance renewals and installs as appropriate managed by Successful Respondent.

**Type:**

R

**Applicable Service Component(s)**

Security Operations Services, MSI, TBD

**Definition:** This SLA includes the renewal and installation of software licenses (including infrastructure stack and DCS Customer “Software Services Charge” software) included in the Agreement and hardware maintenance agreements included in the Agreement and DCS Customer Hardware Service Charges (HSC).

The Service Level calculation for “License and Maintenance Renewal Timeliness” is the total number of license or maintenance renewals processed and installed as appropriate prior to their expiration divided by the total number of license or maintenance agreements scheduled to expire within the Measurement Window.

For months in which the total volume of license renewals is low, such that missing two (2) or more renewals would result in a miss of a Minimum Service Level target

Successful Respondent will provide current proof of entitlements, license renewal dates, and maintenance renewal dates to the MSI. Data will be maintained in the MSI Contract Management Module. A License and Maintenance Renewal Report will compare renewals that are due in the Measurement Window against those that met or failed the target renewal date.

Software and hardware renewals and software installations as appropriate will be logged and tracked in the MSI ITSM system. Successful Respondent will receive a Service Request to renew from the MSI ITSM system.

When appropriate a Change Request will be issued to install software. Software renewal installations will be categorized and assigned to resolver teams who will work to fulfill the request.

Software and hardware renewal data will be uploaded to the MSI on a daily basis.

**Formula:**

$$\text{License and Maintenance Renewal Timeliness} = \frac{\text{Total Number of License and Maintenance Renewals Processed and Installed on Time}}{\text{Total Number of License and Maintenance Renewals Due to be processed and installed}}$$

**Measurement Window:** Month

**Data Source:** MSI ITSM, MSI Contract Management Module

**Frequency of Collection:** Monthly

## 2.7 Invoice Dispute Resolution

**Business Intent:** Disputes for invoices are addresses promptly and amicably to all parties to the extent possible and do not otherwise add unanticipated duration or complexity to Customer invoicing and payment processes.

**Type:** R

**Applicable Service Component(s)** Security Operations Services, MSI, TBD

**Definition:** The Service Level calculation for “Invoice Dispute Resolution” is the total number of invoice disputes that are resolved within twenty (20) Business Days of submission, divided by the total number of resolved invoice disputes plus the total number of open invoice disputes that have exceeded twenty (20) Business Days, with the result expressed as a percentage.

For purposes of clarity, note the following:

1. if an invoice dispute is initiated within the current Measurement Window, but the twenty Business Days extends beyond the end of the current Measurement Window, then it is excluded from the current Measurement Window’s calculation (unless such dispute is actually resolved in the current Measurement Window, in which case it is included in the current Measurement Window’s calculation);
2. an open invoice dispute that has exceeded the committed timeframe is also carried forward into subsequent Measurement Windows as a breach until resolved; if it is resolved within twenty-eight (28) days following its relevant committed timeframe, it is excluded from the subsequent Measurement Window; otherwise, it is counted as failed to meet the committed timeframes in each subsequent Measurement Window’s calculation until resolved.

**Formula:**

$$\text{Invoice Dispute Resolution} = \frac{\text{Number Invoice Disputes Resolved within twenty (20) days}}{\text{Total Number of Invoice Disputes plus open Invoice Disputes that should have been resolved}}$$

**Measurement Window:** Month

**Data Source:** MSI IT Financial Management

**Frequency of Collection:** Monthly

## 2.8 Patch Compliance

**Business Intent:** To ensure timely notification and compliance with all security and software patches.

**Type:** U

**Applicable Service Component(s)** Security Operations Services

**Definition:** Measure the percentage of patches (both Security and Software) initiated timely and applied successfully as documented in the DIR’s approved Change Request ticket. Timeliness requirements to initiate a patch are determined as follows (in calendar days):

Time to open CRQ	CVSS Score	If CVSS Score is not available	RedHat	Microsoft Non-Security	Microsoft Security	Oracle	Other
1 Day	≥ 9.0	:	Critical	Critical	Critical	Alert	Critical
3 Days	7.0 - 8.9		Important		Important	Critical	
7 Days	4.0 - 6.9		Moderate	Non-Critical	Moderate	Bulletin	Non-Critical / Uncategorized
14 Days	< 4.0		Low		Low		

Timeliness measurement is based on the time the patches are received from the vendor to the time the change request ticket to the Customer is created.

Scheduled hours of operations and maintenance windows for each infrastructure element will be maintained in the SMM. Changes are not successfully implemented if they: (i) do not comply with the Change Management procedures (including the Change Control Process) and the SMM; (ii) cause either a Severity 1 Incident or Severity 2 Incident; (iii) exceed the change window; (iv) are backed out; or (v) partial success of change is backed out or unsuccessful.

Patches not approved by DIR for implementation are excluded from this SLA.

**Formula:**

$$\text{Patch Compliance} = \frac{\text{Total number of Patch CRQs initiated within the required timeframes and applied successfully}}{\text{Total Number of Patches initiated and applied plus number of patches that should have been initiated and applied}}$$

**Measurement Window:** Monthly

Change tickets will be logged in the MSI ITSM system. Changes will be documented, categorized, and assigned to implementer teams who will work to plan, review, obtain approvals, and progress the ticket through the change management lifecycle.

**Data Source:** Change data will be uploaded to ServiceFlow on a daily basis. ServiceFlow will filter change tickets based on appropriate measurement criteria.

**Frequency of Collection:** Per Patch Implementation Request. Twenty-four (24) hours a day, seven (7) days a week, 365 days a year

### 3 Key Performance Indicators

This Section sets forth qualitative descriptions of the Key Performance Indicators (KPIs). 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.

#### 3.1 Shared Services Growth

Table 2: Shared Services Growth KPI

Key Performance Indicator Name	
<b>Shared Services Growth</b>	
<b>KPI DESCRIPTION and PURPOSE</b>	The KPI “Shared Services Growth” provides a metric against overall growth in DIR’s Shared Services. The measurement is based on a composite of growth in number of Customers, growth in Shared Services volume, and growth in number of discrete Services offered, growth in shared services spend per Customer, and growth in shared service spend outside state agencies.
<b>ALGORITHM</b>	<p>The calculation for “Shared Services Growth” includes five (5) different calculations, one (1) for each of its respective Operating Measures (OM), each producing a 1-5 numeric rating. These five (5) numeric ratings will then be weighted and averaged together per the weight for each OM:</p> <p><u>4.9</u>: Growth in number of Customers:                      &lt; 0% = 1                      ≥ 0 - &lt; 5% = 2                      ≥ 5 - &lt; 10% = 3                      ≥ 10 - &lt; 15% = 4                      ≥ 15% = 5</p> <p><u>4.10</u>: Growth in Shared Services Volume:                      &lt; 0% = 1                      ≥ 0 - &lt; 5% = 2                      ≥ 5 - &lt; 10% = 3                      ≥ 10 - &lt; 15% = 4                      ≥ 15% = 5</p> <p><u>4.11</u>: Growth in number of Services offered:                      ≤ 0 = 1                      1 = 2                      2 = 3                      3 = 4                      ≥ 4 = 5</p> <p><u>4.12</u>: Growth in Shared Services spend per Customer                      &lt; 0% = 1                      ≥ 0 - &lt; 5% = 2                      ≥ 5 - &lt; 10% = 3                      ≥ 10 - &lt; 15% = 4                      ≥ 15% = 5</p> <p><u>4.13</u>: Growth in Shared Services spend by Customers other than State Agencies:                      &lt; 0% = 1                      ≥ 0 - &lt; 5% = 2                      ≥ 5 - &lt; 10% = 3                      ≥ 10 - &lt; 15% = 4                      ≥ 15% = 5</p>
<b>DATA SOURCES AND COLLECTION PROCESS</b>	<p>Number of Customers, Resource Units, and consumption (spend) data will be sourced from the Digital MSI IT Financial Management system. Service Offerings will be sourced from the MSI Service Management system.</p> <p>Data will be loaded to the Digital MSI Analytics platform a regular basis. Month over month change in each of the Operating Measure components will be calculated as defined in the Operating Measurements and rated against the respective component targets. The individual component ratings will be aggregated into a single, overall result based on pre-defined weightings.</p>
<b>REPORTING TOOLS</b>	Digital MSI Analytics platform Digital MSI IT Financial Management system Digital MSI Service Management system
<b>RAW DATA STORAGE (ARCHIVES)</b>	Data will be available on line, and archived, per agreed data retention policies.
<b>KPI REPORTING</b>	<input type="checkbox"/> Daily

Key Performance Indicator Name	
	<input checked="" type="checkbox"/> Monthly <input type="checkbox"/> Quarterly <input type="checkbox"/> Semi Annual

3.2 Customer Satisfaction

Table 3: Customer Satisfaction KPI

Key Performance Indicator Name	
<b>Customer Satisfaction</b>	
<b>KPI DESCRIPTION and PURPOSE</b>	The KPI “Customer Satisfaction” provides a metric against overall Customer Satisfaction. The measurement is based on a composite of Customers surveyed as “Satisfied” for both Executive level and Operational level, monthly Customers scorecard rating of acceptable, monthly Customer service desk survey, and monthly constituent portal and application survey.
<b>ALGORITHM</b>	The calculation for “Customer Satisfaction” includes four (4) different calculations, each producing a 1-5 numeric rating. These four (4) numeric ratings will then be weighted, then averaged together per the weight for each OM: <u>4.14:</u> Percentage Customers “Satisfied,” Executive Level: < 75% = 1 ≥ 75 - < 85% = 2 ≥ 85 - < 90% = 3 ≥ 90 - < 95% = 4 ≥ 95% = 5 <u>4.14:</u> Percentage Customers “Satisfied,” Operational Level: < 75% = 1 ≥ 75 - < 85% = 2 ≥ 85 - < 90% = 3 ≥ 90 - < 95% = 4 ≥ 95% = 5 <u>4.15:</u> Monthly Customer scorecard: < 75% = 1 ≥ 75 - < 85% = 2 ≥ 85 - < 90% = 3 ≥ 90 - < 95% = 4 ≥ 95% = 5 <u>4.16:</u> Customer service desk survey: < 75% = 1 ≥ 75 - < 85% = 2 ≥ 85 - < 90% = 3 ≥ 90 - < 95% = 4 ≥ 95% = 5
<b>DATA SOURCES AND COLLECTION PROCESS</b>	Executive Level and Operational Level Survey data will be obtained via annual survey conducted by an independent, DIR approved third-party. Customer Scorecard survey data measuring satisfaction with MSI and SCP services will be sourced from the Digital MSI Service Management system. Service Desk survey data will be obtained from the Digital MSI Service Management system survey tool, administered upon completion a request or resolution of an Incident. Constituent Portal and Constituent Portal Application satisfaction data will be obtained from survey data supplied by the texas.gov SCPs.  Data will be loaded to the Digital MSI Analytics platform a regular basis. Performance results for the annual Executive and Operational Level satisfaction survey will be calculated as defined in the Operating Measurements and rated against respective component targets. Month over month change in Service Desk, SCP Delivery of Shared Services, Constituent Portal and Constituent Application Customer Satisfaction will calculated as defined in the Operating Measurements and rated against respective component targets. The individual

Key Performance Indicator Name	
	component ratings will be aggregated into a single overall, result based on pre-defined weightings.
REPORTING TOOLS	Digital MSI Analytics platform Digital MSI Service Management system survey tool SCP Survey tools 3 <sup>rd</sup> Party Survey tools
RAW DATA STORAGE (ARCHIVES)	Data will be available on-line, and archived, per agreed data retention policies.
KPI REPORTING	<input type="checkbox"/> Daily <input type="checkbox"/> Monthly <input type="checkbox"/> Quarterly <input type="checkbox"/> Semi Annual <input checked="" type="checkbox"/> As defined by unique OM above

3.3 Service Quality

Table 4: Service Quality KPI

Key Performance Indicator Name	
<b>Service Quality</b>	
KPI DESCRIPTION and PURPOSE	The KPI “Service Quality” provides a metric against general quality of service. The measurement is based on a composite of Service Levels meeting expected targets, measure of processes wholly or substantially automated, percentage change in the number of major incidents, average Service Request fulfillment (in number of applicable days), and percentage of software at n-2 and hardware less than five (5) years old.
ALGORITHM	<p>The calculation for “Service Quality” includes six different calculations, one (1) for each of its six (6) Operating Measures (OM), each producing a 1-5 numeric rating. These six (6) numeric ratings will then be weighted and are then averaged together per the weight for each OM:</p> <p><b>4.19:</b> Percentage of service levels meeting “Expected” target:                      &lt; 75% = 1                      ≥ 75 - &lt; 85% = 2                      ≥ 85 - &lt; 90% = 3                      ≥ 90 - &lt; 95% = 4                      ≥ 95% = 5</p> <p><b>4.21:</b> Percentage of processes wholly or substantially automated:                      &lt; 25% = 1                      ≥ 25 - &lt; 35% = 2                      ≥ 35 - &lt; 45% = 3                      ≥ 45 - &lt; 55% = 4                      ≥ 55% = 5</p> <p><b>4.1:</b> Percentage of change in number of major incidents:                      &gt; 25% = 1                      &gt; 0 - ≤ 25% = 2                      0% = 3                      &lt; 0 - ≤ -25% = 4                      &lt; -25% = 5</p> <p><b>4.20:</b> Service request fulfillment in average number of Business Days:                      ≥ 35 = 1                      ≥ 30 - &lt; 35 = 2                      ≥ 25 - &lt; 30 = 3</p>

Key Performance Indicator Name	
	<p>≥ 20 - &lt; 25 = 4</p> <p>&lt; 20 = 5</p> <p><u>4.22</u>: Percentage of software at or above n-2:</p> <p>&lt; 75% = 1</p> <p>≥ 75 - &lt; 85% = 2</p> <p>≥ 85 - &lt; 90% = 3</p> <p>≥ 90 - &lt; 95% = 4</p> <p>≥ 95% = 5</p> <p><u>4.24</u>: Percentage of hardware less than five (5) years old:</p> <p>&lt; 75% = 1</p> <p>≥ 75 - &lt; 85% = 2</p> <p>≥ 85 - &lt; 90% = 3</p> <p>≥ 90 - &lt; 95% = 4</p> <p>≥ 95% = 5</p>
<b>DATA SOURCES AND COLLECTION PROCESS</b>	<p>The number of Critical and Key Service Levels meeting or exceeding the Expected Service Level will be obtained from the Digital MSI Service Level Management Reporting system when the final monthly Service Level Report is published. Data for in-scope processes will be obtained from the SMM. Data for level of process automation will be based an assessment of level of automation. Number of Major Incidents and the average number of Business Days to fulfill Service Requests will be sourced from the Digital MSI Service Management system. Software at N-2 or higher, and hardware less than five (5) years old will be sourced from the Digital MSI CMDB.</p> <p>Data will be loaded to the Digital MSI Analytics platform a regular basis. Values for each component, as defined in the Operational Measurements will be calculated and rated against respective component targets. The individual components ratings will be aggregated into a single, overall result based on pre-defined weightings.</p>
<b>REPORTING TOOLS</b>	<p>Digital MSI Analytics platform</p> <p>Digital MSI IT Service Level Management system</p> <p>Digital MSI Service Management system</p> <p>Digital MSI CMDB</p> <p>MSI Service Management Manual</p>
<b>RAW DATA STORAGE (ARCHIVES)</b>	<p>Data will be available on-line, and archived, per agreed data retention policies.</p>
<b>KPI REPORTING</b>	<p><input type="checkbox"/> Daily</p> <p><input checked="" type="checkbox"/> Monthly</p> <p><input type="checkbox"/> Quarterly</p> <p><input type="checkbox"/> Semi Annual</p>

3.4 Value

Table 5: Value KPI

Key Performance Indicator Name
Value

Key Performance Indicator Name	
<b>KPI DESCRIPTION and PURPOSE</b>	<p>The KPI “Value” provides a metric against overall value for the money, partially relying on a quarterly repository of third-party market data as an industry benchmark. The measurement is based on a composite of percentage of spend within the market range, percentage of automated service requests offered through the Service Catalog, and percentage of Customers satisfied with service offerings.</p> <p><b>NOTE:</b> this does not constitute a benchmark in terms of invoking any form of contractual remedy.</p>
<b>ALGORITHM</b>	<p>The calculation for “Value” includes three different calculations, one (1) for each of its three (3) OMs, each producing a 1-5 numeric rating. These three (3) numeric ratings will then be weighted and are then averaged together per the weight for each OM:</p> <p><a href="#">4.25:</a> Percentage of Services offered where spend is within market range:</p> <ul style="list-style-type: none"> <li>&lt; 60% = 1</li> <li>≥ 60 - &lt; 70% = 2</li> <li>≥ 70 - &lt; 80% = 3</li> <li>≥ 80 - &lt; 90% = 4</li> <li>≥ 90% = 5</li> </ul> <p><b>NOTE:</b> spend is either within market range or not within market range as measured for each respective service, compared against most similar available data.</p> <p><a href="#">4.26:</a> Percentage of automated service requests offered self-provisioned through Service Catalog:</p> <ul style="list-style-type: none"> <li>&lt; 50% = 1</li> <li>≥ 50 - &lt; 60% = 2</li> <li>≥ 60 - &lt; 70% = 3</li> <li>≥ 70 - &lt; 80% = 4</li> <li>≥ 80% = 5</li> </ul> <p><a href="#">4.2:</a> Percentage of Customers satisfied with service offerings</p> <ul style="list-style-type: none"> <li>&lt; 60% = 1</li> <li>≥ 60 - &lt; 70% = 2</li> <li>≥ 70 - &lt; 80% = 3</li> <li>≥ 80 - &lt; 90% = 4</li> <li>≥ 90% = 5</li> </ul>
<b>DATA SOURCES AND COLLECTION PROCESS</b>	<p>Shared Services spend will be sourced from the Digital MSI IT Financial Management system. Quarterly comparable market survey data will be obtained via an external, DIR approved benchmarking service. Number of automated Service Requests offered will be obtained from the Digital MSI IT Service Management system. Customer satisfaction with Service Offerings will be obtained via an annual survey conducted by an independent, DIR approved third-party.</p> <p>Data will be loaded to the Digital MSI Analytics platform a regular basis. Values for each component, as defined in the Operating Measurements will be calculated and rated against respective component targets. The individual components ratings will be aggregated into a single, overall result based on pre-defined weightings.</p>
<b>REPORTING TOOLS</b>	<p>Digital MSI Analytics platform                      Digital MSI IT Financial Management system                      Digital MSI Service Management system</p>
<b>RAW DATA STORAGE (ARCHIVES)</b>	<p>Data will be available on-line, and archived, per agreed data retention policies.</p>

Key Performance Indicator Name	
<b>KPI REPORTING</b>	<input type="checkbox"/> Daily <input checked="" type="checkbox"/> Monthly <input type="checkbox"/> Quarterly <input type="checkbox"/> Semi Annual

3.5 Security

Table 6: Security KPI

Key Performance Indicator Name	
<b>Security</b>	
<b>KPI DESCRIPTION and PURPOSE</b>	The KPI “Security” provides a metric against the measure of Security the DIR shared services are offering. The measurement is based on a composite of percentage of change in number of major security incidents, change in risk based on vulnerability scan measures, change in annual Common Security Framework (CSF) Maturity rating, and change in the number of devices monitored by SIEM/Security Analytical Devices.
<b>ALGORITHM</b>	The calculation for “Security” includes four different calculations, one (1) for each of its four (4) OMs, each producing a 1-5 numeric rating. These four (4) numeric ratings will then be weighted and are then averaged together per the weight for each OM:  <b>4.30:</b> Percentage change in number of major security incidents: $> 25\% = 1$ $> 0 - \leq 25\% = 2$ $0\% = 3$ $< 0 - \leq -25\% = 4$ $< -25\% = 5$  <b>4.27:</b> Percentage change in risk based on vulnerability scan measure: $> 25\% = 1$ $> 0 - \leq 25\% = 2$ $0\% = 3$ $< 0 - \leq -25\% = 4$ $< -25\% = 5$  <b>4.28:</b> Percentage change in Annual CSF Maturity Rating: $< -25\% = 1$ $\geq -25 - < 0\% = 2$ $0\% = 3$ $\leq 25 - > 0\% = 4$ $> 25\% = 5$  <b>4.29:</b> Percentage of security devices monitored by SEIM/Security Analytical Devices: $< 70\% = 1$ $\geq 70\% - < 80\% = 2$ $\geq 80\% - < 90\% = 3$ $\geq 90\% - < 99\% = 4$ $\geq 99\% = 5$

Key Performance Indicator Name	
<b>DATA SOURCES AND COLLECTION PROCESS</b>	<p>Number of major Security Incidents will be sourced from the Digital MSI Service Management system. Risk ratings based on vulnerability scans will be sourced from data provided from the MSI and SCP scanning tools as uploaded by the MSI and SCPs. Number of devices monitored by SEIM/Security Analytical Devices will be provided by the SCPs and loaded into the Digital MSI Service Management system. Maturity of Common Security Framework (CSF) Rating will be as documented in the Annual Security Plan.</p> <p>Data will be loaded to the Digital MSI Analytics platform a regular basis. Month over month change for Major Incidents, vulnerability risk ratings and Monitored Devices will be calculated as defined in the Operating Measurements and rated against respective component targets. Annual change for maturity of CSF Rating will be calculated and rated against the relevant target. The individual component ratings will be aggregated into a single, overall result based on pre-defined weightings.</p>
<b>REPORTING TOOLS</b>	<p>Digital MSI Analytics platform</p> <p>DIR SPECTRIM</p> <p>Digital MSI Service Management System</p> <p>MSI Annual Security Plan</p>
<b>RAW DATA STORAGE (ARCHIVES)</b>	<p>Data will be available on-line, and archived, per agreed data retention policies.</p>
<b>KPI REPORTING</b>	<p><input type="checkbox"/> Daily</p> <p><input checked="" type="checkbox"/> Monthly</p> <p><input type="checkbox"/> Quarterly</p> <p><input type="checkbox"/> Semi Annual</p>

#### 4 OPERATING MEASUREMENTS

This Section sets forth qualitative descriptions of the OMs. The business objectives and commencement of obligations associated with such Operating Measurements are set forth in **Attachment 1.2 Service Level Matrix**.

To ensure visibility of progress toward business and strategic objectives, the Successful Respondent will report Operating Measurements.

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.

##### 4.1 Percentage of change in number of Major Incidents

The purpose of this measure is to track the change in the number of Major Incidents over time.

The calculation for “Percentage Change in Number of Major Incidents” is the change in the number of Major Incidents within a given Measurement Window, divided by the number of Major Incidents for the previous Measurement Window, reported as a percentage.

##### 4.2 Percentage of Customers satisfied with service offerings

The purpose of this measure is to track the percentage of DIR Customers who report as being “Satisfied” with the service offerings.

The calculation for “Percentage of Customers satisfied with service offerings” is the number of DIR Customers who respond to the standard administered satisfaction survey with a score associated with a “Satisfied” or higher, divided by the total number of Customers who responded to the survey for the same Measurement Window.

##### 4.3 Problem: Time to Review and Deliver RCA

The purpose of this measure is to track how long it takes to review and deliver a RCA to the responsible party.

The calculation for “Time to Review and Deliver RCA” is, for a given Measurement Window, the total number of RCAs Reviewed and Delivered within the committed timeframes by the Successful Respondent, divided by the total number of RCAs scheduled to be Reviewed and Delivered by the Successful Respondent during such Measurement Window, with the result expressed as a percentage.

#### 4.4 Asset: Assets Updated by eDiscovery

The purpose of this measure is to determine how often the asset database is updated based on eDiscovery.

The calculation for “Assets Updated by eDiscovery” is, for a given Measurement Window, the total number of asset records updated by eDiscovery, divided by the total number of asset records updated during such Measurement Window, with the result expressed as a percentage.

#### 4.5 Asset: Asset Attributes Updated Electronically

The purpose of this measure is to determine how often the asset attribute fields of the asset database are updated electronically.

The calculation for “Asset Attributes Updated Electronically” is, for a given Measurement Window, the total number of attributes of asset records updated via automated data feeds divided by the total number of attributes of asset records updated during such Measurement Window, with the result expressed as a percentage.

#### 4.6 Invoicing: Invoice Delivered On-time

The purpose of this measure is to determine how often the invoices are delivered to DIR on-time.

The calculation for “Invoice Delivered On-time” is, for a given Measurement Window, the total number of delivered and Accepted Invoices within the committed timeframes, divided by the total number of Invoices scheduled to be delivered during such Measurement Window, with the result expressed as a percentage.

#### 4.7 Invoicing: Time to Assign Invoice Dispute

The purpose of this measure is to track how long it takes to assign an invoice dispute to the responsible party.

The calculation for “Time to Assign Invoice Dispute” is, for a given Measurement Window, the total number of Invoice Dispute tickets assigned by the MSI to the responsible SCP within the committed timeframes, divided by the total number of Invoice Dispute tickets assigned by the MSI to the responsible SCPs during such Measurement Window, with the result expressed as a percentage.

#### 4.8 Devices Reporting via Electronic Management Tool

The purpose of this measure is to measure the percentage of managed Devices reporting via electronic management tools.

The calculation for “Devices Reporting via Electronic Management Tool” is the number of managed Devices reporting via electronic management tools that are correctly reporting during the applicable Measurement Window, divided by the total number of managed Devices that should be reporting during the applicable Measurement Window, with the result expressed as a percentage.

#### 4.9 Growth in Number of Customers

The purpose of this measure is to measure the growth in DIR Customers.

The calculation for “Growth in Number of Customers” is the increase in number of Customers for a given Measurement Window, divided by the number of Customers at the at the end of the previous Measurement Window, with the result expressed as a percentage.

#### 4.10 Growth in Shared Services Volume

The purpose of this measure is to measure the growth in adoption of DIR Shared Services, as indicated in the normalized change in Shared Services Volume.

The calculation for “Growth in Shared Services Volume” is the change in total volume of services consumed, as defined by Resource Units, against all Shared Services Programs for a given Measurement Window, divided by the total volume of services consumed, as defined by Resource Units, against all Shared Services Programs for the previous Measurement Window, expressed as a percentage. Volumes normalized to account for anomalies or unusual one-time events; exclude Hardware Service Charges and Software Service Charges.

#### 4.11 Growth in Number of Services Offered

The purpose of this measure is to measure the growth in the number of discrete Services offered to DIR Customers or potential Customers.

The calculation for “Growth in Number of Services Offered” is the number of discrete Services offered at the end of a given Measurement Window, minus the total number of discrete Services offered at the end of the previous Measurement Window.

#### 4.12 Growth in Shared Services Spend per Customer

The purpose of this measure is to measure the value of the services offered by DIR to wide Customer base and the success of the outreach plans in driving penetration in various Customer segments.

The calculation for “Growth in Shared Services Spend per Customer” is the change in the average Shared Services Spend per Customer divided by the average Shared Services Spend per Customer from the previous Measurement Window, expressed as a percentage.

#### 4.13 Growth in Shared Services Spend by Customers other than State Agencies

The purpose of this measure is to measure the increase in service adoption for DIR eligible customers outside of State Agencies.

The calculation for "Growth in Shared Services Spend by Customers other than State Agencies" is the change in the total Shared Services Spend of Non-State Agency Customer divided by the total Shared Services Spend of Non-State Agency Customers from the previous Measurement Window, expressed as a percentage.

#### 4.14 Percentage of Executive/IT Operational Staff Customers Satisfied

The purpose of this measure is to track the percentage of DIR Customers who report as being “Satisfied” (or higher).

The calculation for “Percentage of Customers Satisfied” is the number of DIR Customers, both at the Executive and Operational Levels who respond to the standard administered satisfaction survey with a score associated with a “Satisfied” or higher, divided by the total number of Customer, both at the Executive and Operational Level, who responded to the survey for the same Measurement Window.

#### 4.15 Monthly Customer Scorecard – **Acceptable**

The purpose of this measure is to track the overall Customer sentiment regarding the delivery of all shared services.

The calculation for "Monthly Customer Scorecard" is the change in the number of Customer responses that resulted in a rating of Acceptable or higher over total number of Customer responses, expressed as a percentage, from the previous measurement window.

#### 4.16 Customer Service Desk Survey

The purpose of this measure is to track the effectiveness of the customer service desk for all shared services.

The calculation for " Customer Service Desk Survey" is the change in the number of customer responses that resulted in a rating of Acceptable or higher over the total number of customer service desk survey responses, expressed as a percentage, from the previous measurement window.

#### 4.17 <INTENTIONALLY LEFT BLANK>

<INTENTIONALLY LEFT BLANK>

#### 4.18 <INTENTIONALLY LEFT BLANK>

<INTENTIONALLY LEFT BLANK>

#### 4.19 Percentage of Service Levels Meeting Expected Targets

The purpose of this measure is to track the percentage of Service Levels that achieve their Expected Target or better.

The calculation for “Percentage of Service Levels Meeting Expected Targets” is the number of Services Levels that achieve their Expected Target or better for a given Measurement Window, divided by the total number of Service Levels in effect during that same Window.

#### 4.20 Service Request Fulfillment in Days

The purpose of this measure is to measure the number of Business Days required to fulfill a normal Customer Service Request, per the timeframes used to measure the Service Request Fulfillment Service Level.

The calculation for “Service Request Fulfillment in Days” is the average number of Business Days from the creation of a Customer Service Request to the point the Request is completed, expressed in number days.

#### 4.21 Percentage of Automated Processes

The purpose of this measure is to monitor the percentage of in-scope processes that are substantially or wholly automated. This is intended to reflect the achievement of DIR’s envisioned “Digital MSI”.

The calculation for “Percentage of Automated Processes” is the number of in-scope processes which are wholly or substantially automated, divided by the total number of in-scope processes, expressed as a percentage. The Service Management Manual will serve as a reference for identifying the in-scope processes.

#### 4.22 Percentage of Software at N-2 or Higher

The purpose of this software currency measure is to monitor the overall quality of the Shared Service offered by measuring the extent of technological innovations through upgrades to software.

The calculation for “Percentage of Software at N-2 or Higher” is the number of software assets in the CMDB that are at N-2 or Higher over the total number of software assets in the CMDB, expressed as a percentage.

#### 4.23 Percentage of Software that is Supported

The purpose of this software currency measure is to monitor the overall quality and security of the Shared Service offered by measuring the extent of all software that is supported by the manufacturer.

The calculation for “Percentage of Software that is Supported” is the number of software assets in the CMDB that are at supported over the total number of software assets in the CMDB, expressed as a percentage.

#### 4.24 Percentage of Hardware Less Than Five (5) Years Old

The purpose of this measure is to monitor the overall quality of the Shared Service offered by measuring the reliability and currency of hardware.

The calculation for “Percentage of Hardware Less Than 5 Years Old” is the number of hardware assets in the CMDB that are less than five (5) years old over the total number of hardware assets in the CMDB, expressed as a percentage.

#### 4.25 Percentage of Spend within Market Range

The purpose of this measure is to track the percentage of Program spend that is within five percent of the market range for comparable service.

The calculation for “Percentage of Spend within Market Range” is the sum of all Shared Service spend against Shared Services that are within five percent of their respective comparable market range for that service, divided by the total of all Shared Services spend, expressed as a percentage.

**NOTE:** spend is either within market range or not within market range as measured for each respective service, compared against most similar available data. The calculation should only capture spend where the Successful Respondent has comparable market data.

#### 4.26 Percentage of Service Requests Self-Provisioned Through Service Catalog

The purpose of this measure is to monitor the efficiency of service delivery by measuring the amount of shared services procured through an automated marketplace, with little to no additional intervention from SCP or Successful Respondent personnel.

The calculation for "Percentage of Service Requests Self-Provisioned Through Service Catalog" is the number of Service Requests procured through an automated process via the Service Catalog divided by the number of Service Requests procured via the Service Catalog for that measurement window, expressed as a percentage.

#### 4.27 Change in Risk Based on Vulnerability Scan Measures

The purpose of this measure is to monitor the security risk of the state by way of measuring the number of vulnerabilities identified through vulnerability scans.

The calculation for "Change in Risk Based on Vulnerability Scan Measures" is identifying the change in the results of the following formula compared to the previous measurement window, expressed as a percentage:  $(\text{Multiplier of critical x defects}) + (\text{Multiplier of high x defects}) + (\text{Multiplier of medium x defects}) + (\text{Multiplier of low x defects})$

Overall risk is based on multipliers for each severity of defect. Level of vulnerabilities tracked and measured will be specified in the SMM.

#### 4.28 Change in Annual Common Security Framework (CSF) Maturity Rating

The purpose of this measure is to monitor the effectiveness of the various security measures deployed in maturing the state's security posture, by way of comparing the previous year's security posture to the most recent CSF Rating.

The calculation for "Change in Annual CSF Maturity Rating" is the change in the most current Annual CSF Maturity Rating divided by the previous year's Annual CSF Maturity Rating, expressed as a percentage.

#### 4.29 Percentage of Security Devices monitored by Security Incident and Event Management (SIEM)/Security Analytical Devices

The purpose of this measure is to monitor the extent by which the deployed security devices in the DCS environment are monitored by security tools and reporting into a SIEM; therefore, enhancing the overall security posture for the state.

The calculation for "Percentage of Security Devices monitored by SIEM/Security Analytical Devices" is the number of devices monitored and reporting to a SIEM over the total number of devices monitored in the environment, expressed as a percentage.

#### 4.30 Percentage Change in Number of Major Security Incidents

The purpose of this measure is to track the change in the number of major Security Incidents over time.

The calculation for "Percentage Change in Number of Major Security Incidents" is the change in the number of major Security Incidents within a given Measurement Window, divided by the number of major Security Incidents for the previous Measurement Window, reported as a percentage.

## 5 OPERATIONAL REPORTS

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

1. Providing all Reports currently being provided by the Incumbent Successful Respondent, including:
  - a. Those Reports listed in **Appendix A Reports**, including those reports contemplated in **Appendix A**, 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 reports development process (e.g., requirements, development, test, acceptance, production ready) to be completed for each designated Report prior to the Commencement Date.
2. 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 DIR Customers to request Reports based on standard data provided via the Portal or **Exhibit 1 Statement of Work**, as applicable.

- b. Provide capability for DIR or DIR Customer to generate ad hoc reports via the reporting tool.
3. Delivering all Reports requested within other documents that are referenced as requirements in other Exhibits.
  - a. In compliance with report specifications identified in a formal reports development process (e.g., requirements, development, test, acceptance, production ready) to be completed for each designated Report prior to Commencement Date.
4. Modifying the format, content, and frequency of any Report as requested by DIR during the Term, subject to Change Management procedures.
5. At a minimum, provide all Reports via the Portal through a real-time web-accessible reporting dashboard.
6. Provide access statistics for Reports presented via the Portal at the request of DIR.
7. Providing soft or hard copies of Reports as requested by DIR.