

Appendix 4 to
Seventh Amendment of
Master Services Agreement

Exhibit 3-B
SLA Definitions, Tools, Methodologies

DIR-MSS-SCP-001

August 10, 2020



**Exhibit to Managed Security Services
Service Component Provider
Master Services Agreement**

DIR Contract No. DIR-MSS-SCP-001

Between

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

and

AT&T Corp.

**Attachment 3-B
SLA Tools, Definitions, Methodologies**

August 10, 2020

Change Log			
CCR/CN	Amendment	Date	Description
CCR-000309		09/19/2018	<ul style="list-style-type: none"> • Clarifies A.5.6. Patch Compliance - Managed Devices - Modification of Wording
CCR-000329	Amendment 2	12/12/2018	<ul style="list-style-type: none"> • Updates the descriptions of the SLAs to align with MSI contract
CCR-000350	Amendment 4	6/26/2019	<ul style="list-style-type: none"> • Adds definition for “Availability” in Section 7.2 for DIR's Statewide Portal for Enterprise Cybersecurity Threat, Risk and Incident Management (SPECTRIM) system for local government entities.
CCR-000XXX	Amendment 7	8/10/2020	<ul style="list-style-type: none"> • Removes definition for “Availability” in Section 7.2 for DIR's Statewide Portal for Enterprise Cybersecurity Threat, Risk and Incident Management (SPECTRIM) system for local government entities.

TABLE OF CONTENTS

A.0	CRITICAL SERVICE LEVELS – MANAGED SECURITY	1
A.1	Solution Proposal Delivery	1
A.2	Solution Implementation.....	4
A.3	Invoice Dispute Resolution	6
A.4	Report Delivery.....	7
A.5	Service Area Service Levels – Security Monitoring & Device Management.....	9
A.6	Service Area Service Levels – Incident Response	23
A.7	Service Area Service Levels – Risk & Compliance.....	27
B.0	KEY MEASUREMENTS – MANAGED SECURITY	29
B.1	Root Cause Analysis Delivery	29
B.2	Corrective Actions	30
B.3	Resolution Time – Severity Level 1, 2, 3 and 4.....	32
B.4	Service Request Fulfillment.....	34
B.5	Change Management Effectiveness	36

A.0 CRITICAL SERVICE LEVELS – MANAGED SECURITY

This Section sets forth qualitative descriptions of the Critical Service Levels for the Managed Security Services Service Components. The numerical Minimum Service Levels, Expected Service Levels and commencement of obligations associated with such Critical Service Levels are set forth in **Attachment 3-A** Service Level Matrix. Critical Service Levels A.1 through A.4 are common to all Service Components.

A.1 Solution Proposal Delivery

SERVICE LEVEL NAME	EXHIBIT NUMBER	SECTION REFERENCE	START DATE
Solution Proposal Delivery – Security Monitoring & Device Management Solution Proposal Delivery – Incident Response Solution Proposal Delivery – Risk & Compliance	3-A	1.1.11	
SERVICE LEVEL TYPE	Critical Service Level		
CURRENTLY MEASURED	Yes		
SERVICE COMPONENT(S)	Security Monitoring & Device Management, Incident Response, Risk & Compliance		

<p>METRIC DESCRIPTION</p>	<p>The Service Level for “Solution Proposal Delivery” measures the percentage of time Service Provider delivers a viable proposal to DIR Customers within the committed timeframes in response to a solution request.</p> <p>Following validation of requirements, the Service Provider shall deliver a proposal for each request within the established timeframes, as maintained in the SMM.</p> <p>When a proposal is delivered, it must include a committed solution delivery date in alignment with established Service Levels. This committed number of Business Days will be tracked in the “Solution Implementation” Service Level.</p> <p>Specific size criteria and guidelines shall be maintained in the SMM.</p> <p>Requests are worked in the approved prioritization order of the Customer. Following validation of requirements by the PMO team, the Service Provider shall deliver a proposal for each request within the timeframes as listed below:</p> <ul style="list-style-type: none"> • Extra Small within 1 business day • Small within 11 business days • Medium within 22 business days • Large within 33 business days • Very Large within 44 business days <p>For <u>Digital Forensics</u> and <u>Incident Management</u> the Service Level is 1 Business Day.</p>
<p>METRIC INCLUSIONS and DATA SOURCES</p>	<p>Each proposal submitted to DIR 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.</p>
<p>METRIC EXCLUSIONS</p>	<p>Service Requests</p>
<p>HOURS OF MEASUREMENT</p>	<p>24</p>
<p>DAYS OF MEASUREMENT</p>	<p>365(366)</p>
<p>MINIMUM SERVICE LEVEL</p>	<p>95.00%</p>
<p>EXPECTED SERVICE LEVEL</p>	<p>98.00%</p>

ALGORITHM	<p>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.</p> <p>For purposes of clarity, note the following:</p> <p>(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)</p> <p>(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.</p>
COLLECTION PROCESS	<p>Solution proposal requests will be logged and tracked in the Digital MSI Service Management system as a Service Request. Solution proposal requests will be categorized and assigned to teams who will work to deliver a proposal and progress the ticket through the Request Management lifecycle.</p> <p>Solution proposal data will be uploaded to Digital MSI Service Level Management Reporting system on a daily basis where the Service Level result will be calculated and reported based on appropriate measurement criteria.</p>
REPORTING TOOLS	<ul style="list-style-type: none"> • Digital MSI Service Management system • Digital MSI Service Level Management Reporting system
RAW DATA STORAGE (ARCHIVES)	<p>Data used to calculate the SLA results for reporting will be stored in the Digital MSI Service Level Management Reporting system database, which will be accessible to authorized users via inherent report drill-down functionality for a rolling 13 months. An additional 23 months of data is archived and can be made available via Digital MSI Service Level Management Reporting system upon request by DIR.</p>
PERFORMANCE CATEGORY	Cross Functional
METRIC REPORTING	<input checked="" type="checkbox"/> Monthly <input type="checkbox"/> Quarterly <input type="checkbox"/> Semi Annual

A.2 Solution Implementation

SERVICE LEVEL NAME	EXHIBIT NUMBER	SECTION REFERENCE	START DATE
Solution Implementation – Security Monitoring & Device Management Solution Implementation – Incident Response Solution Implementation – Risk & Compliance	3-A	1.1.12	0
SERVICE LEVEL TYPE	Critical Service Level		
CURRENTLY MEASURED	Yes		
SERVICE COMPONENT(S)	Security Monitoring & Device Management, Incident Response, Risk & Compliance		
METRIC DESCRIPTION	The Service Level for “Solution Implementation” measures the percentage of time Service Provider successfully implements a Solution within the committed timeframe.		
METRIC INCLUSIONS and DATA SOURCES	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.		
METRIC EXCLUSIONS	N/A		
HOURS OF MEASUREMENT	24		
DAYS OF MEASUREMENT	365(366)		
MINIMUM SERVICE LEVEL	95.00%		
EXPECTED SERVICE LEVEL	98.00%		

<p>ALGORITHM</p>	<p>The Service Level calculation for “Solution Implementation” is the total number of requests that are successfully implemented within the committed timeframes, divided by the total number of requests implemented plus the total number of requests that have passed the committed timeframe, with the result expressed as a percentage.</p> <p>Projects will be reported in the Measurement Window in which the associated Project (PPM) ticket is closed, allowing sufficient time to determine if the project was successful.</p> <p>For purposes of clarity, note the following:</p> <p>(a) 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)</p> <p>(b) an uncompleted project is also carried forward into subsequent Measurement Windows as a breach until implemented; if it is implemented 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.</p>
<p>COLLECTION PROCESS</p>	<p>When a solution proposal is approved, a Project (PPM) ticket of type Project will be created by the MSI Program Manager in the Digital MSI Service Management system. Final sign-off documents will be attached by the SCP when the project is accepted as complete. Upon completion of the post implementation review the MSI Program Manager will close the Project (PPM) ticket.</p> <p>Solution implementation data will be loaded to Digital MSI Service Level Management Reporting system on a daily basis where the Service Level result will be calculated and reported based on appropriate measurement criteria.</p>
<p>REPORTING TOOLS</p>	<ul style="list-style-type: none"> • Digital MSI Service Management system • Digital MSI Service Level Management Reporting system
<p>RAW DATA STORAGE (ARCHIVES)</p>	<p>Data used to calculate the SLA results for reporting will be stored in the Digital MSI Service Level Management Reporting system database, which will be accessible to authorized users via inherent report drill-down functionality for a rolling 13 months. An additional 23 months of data is archived and can be made available via Digital MSI Service Level Management Reporting system upon request by DIR.</p>
<p>PERFORMANCE CATEGORY</p>	<p>Cross Functional</p>

METRIC REPORTING	<input checked="" type="checkbox"/> Monthly <input type="checkbox"/> Quarterly <input type="checkbox"/> Semi Annual
-------------------------	---

A.3 Invoice Dispute Resolution

SERVICE LEVEL NAME	EXHIBIT NUMBER	SECTION REFERENCE	START DATE
Invoice Dispute Resolution – Security Monitoring & Device Management Invoice Dispute Resolution – Incident Response Invoice Dispute Resolution – Risk and Compliance	3-A	1.1.13	0
SERVICE LEVEL TYPE	Critical Service Level		
CURRENTLY MEASURED	Yes		
SERVICE COMPONENT(S)	Security Monitoring & Device Management, Incident Response, Risk and Compliance		
METRIC DESCRIPTION	The Service Level for “Invoice Dispute Resolution” measures the percentage of invoice disputes that are resolved within twenty (20) Business Days.		
METRIC INCLUSIONS and DATA SOURCES	N/A		
METRIC EXCLUSIONS	N/A		
HOURS OF MEASUREMENT	8:00 AM – 5:00 PM		
DAYS OF MEASUREMENT	Business Days		
MINIMUM SERVICE LEVEL	93.00%		
EXPECTED SERVICE LEVEL	96.00%		
ALGORITHM	<p>The Service Level calculation for “Invoice Dispute Resolution” is the total number of invoice disputes that are resolved within twenty (20) Business Days of create date in the Digital MSI Service Management system , 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.</p> <p>For purposes of clarity, note the following:</p> <p>(a) 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</p>		

	<p>case it is included in the current Measurement Window's calculation)</p> <p>(b) 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.</p> <p>A low volume alternative calculation, set forth in Exhibit 3 Service Level Matrix, shall apply when the total volume of invoice disputes falls within the volume (denominator) ranges specified in that Exhibit.</p>
COLLECTION PROCESS	<p>Invoice disputes will be logged in ITFM and tracked in the Digital MSI Service Management System as an Invoice Dispute. Invoice Dispute requests will be categorized and assigned to resolver teams who will work to research and resolve the dispute, and progress the request through the Invoice Dispute lifecycle.</p> <p>Invoice Dispute data will be uploaded to Digital MSI Service Level Management Reporting system on a daily basis, where the Service Level result be calculated and reported based on appropriate measurement criteria.</p>
REPORTING TOOLS	<ul style="list-style-type: none"> • Digital MSI Service Management system • Digital MSI Service Level Management Reporting system
RAW DATA STORAGE (ARCHIVES)	<p>Data used to calculate the SLA results for reporting will be stored in the Digital MSI Service Level Management Reporting system database, which will be accessible to authorized users via report drill-down functionality for a rolling 13 months. An additional 23 months of data is archived and can be made available via Digital MSI Service Level Management Reporting system upon request by DIR.</p>
PERFORMANCE CATEGORY	Cross Functional
METRIC REPORTING	<input checked="" type="checkbox"/> Monthly <input type="checkbox"/> Quarterly <input type="checkbox"/> Semi Annual

A.4 Report Delivery

SERVICE LEVEL NAME	EXHIBIT NUMBER	SECTION REFERENCE	START DATE
Report Delivery – Security Monitoring & Device Management	3-A	1.1.14	
Report Delivery – Incident Response			

Report Delivery – Risk and Compliance				
SERVICE LEVEL TYPE	Critical Service Level			
CURRENTLY MEASURED	No			
SERVICE COMPONENT(S)	Security Monitoring & Device Management, Incident Response, Risk and Compliance			
OBJECTIVE	To ensure timely delivery of all reports as required per <u>Attachment 13-A</u>			
METRIC DESCRIPTION	The Service Level for “Report Delivery” measures the percentage of time Service Provider delivers reports per the timeframes identified in <u>Attachment 13-A</u> , Description of Reports.			
METRIC INCLUSIONS and DATA SOURCES	The committed timeframe is that timeframe specified in the <u>Attachment 13-A</u> , Description of Reports, or otherwise as agreed by the requester.			
METRIC EXCLUSIONS	Failure of MSI equipment to be available for delivery of reports. Report delivery failures not reported via an Incident ticket			
HOURS OF MEASUREMENT	24			
DAYS OF MEASUREMENT	365(366)			
MINIMUM SERVICE LEVEL	95.00%			
EXPECTED SERVICE LEVEL	98.00%			
ALGORITHM	The Service Level calculation for “Report Delivery” is the number of Reports delivered on time, divided by the number of Reports scheduled to be delivered during the applicable Measurement Window, with the result expressed as a percentage.			
COLLECTION PROCESS	Tracking and providing information regarding Report Delivery failure will be tracked via Incident tickets created by or on behalf of the customer upon discovery of the missing / incorrect report. The number of Reports delivered on time and the number of Reports scheduled to be delivered will be entered into Digital MSI Service Level Management Reporting system by the MSS SCP via the ITSLM Web Form. Digital MSI Service Level Management Reporting system reports the SLA result based on the Web Form data. Supporting documentation containing details of the data measured and validated will be attached to the Web Form.			

REPORTING TOOLS	As described in the process above, the following tools will be utilized: <ul style="list-style-type: none"> • SCP event monitoring system and tools • Digital MSI Service Management System • MSI CMDB • Digital MSI Service Level Management Reporting system • Service Management Manual • SCP provided dashboard
RAW DATA STORAGE (ARCHIVES)	Data used to calculate the SLA results for reporting will be stored in the Digital MSI Service Level Management Reporting system, which will be accessible to authorized users via inherent report drill-down functionality for a rolling 13 months. An additional 23 months of data is archived and can be made available via Digital MSI Service Level Management Reporting system upon request by DIR.
PERFORMANCE CATEGORY	Other Service Delivery
METRIC REPORTING	<input checked="" type="checkbox"/> Monthly <input type="checkbox"/> Quarterly <input type="checkbox"/> Semi Annual

A.5 Service Area Service Levels – Security Monitoring & Device Management

This Section A.5 shall apply to the Security Monitoring & Device Management Service Component.

This Section sets forth qualitative descriptions of the Critical Service Levels for the Security Monitoring & Device Management Service Component. The numerical Minimum Service Levels, Expected Service Levels and commencement of obligations associated with such Critical Service Levels are set forth in **Attachment 3-A**, CSLs – Monitor & Device Mgmt tab.

A.5.1 Implement New Filters/Signatures

SERVICE LEVEL NAME	EXHIBIT NUMBER	SECTION REFERENCE	START DATE
Implement New Filters/Signatures	3-A	1.1.16	
SERVICE LEVEL TYPE	Critical Service Level		
CURRENTLY MEASURED	No		
SERVICE COMPONENT: AREA(S)	Security Monitoring & Device Management: Endpoint Management Services, IDS/IPS, HIPS, Firewalls, Web Application Firewalls, SIEM, MDS/MPS, SOC Services		
OBJECTIVE	To ensure timely implementation of new filters/signatures		

METRIC DESCRIPTION	Measure the percentage of new filters/signatures successfully implemented within the scheduled change window as documented in the Customer’s approved Change Request ticket.
METRIC INCLUSIONS and DATA SOURCES	Managed Devices are identified in the CMDB. Scheduled hours of operations and maintenance windows for each infrastructure element related to the Managed Device 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), the SMM and, except as specified in clause (ii) to this sentence, (iii) cause either a Severity 1 Incident or Severity 2 Incident, (iv) exceeded the change window, (v) are backed out, or (vi) partial success of change is backed out or unsuccessful.
METRIC EXCLUSIONS	New Filters/Signatures not approved by Customer for implementation
HOURS OF MEASUREMENT	24
DAYS OF MEASUREMENT	365(366)
MINIMUM SERVICE LEVEL	95.00%
EXPECTED SERVICE LEVEL	98.00%
ALGORITHM	The Service Level calculation for “Implement New Filters/Signatures” is the number of changes that are successfully implemented by Service Provider divided by the number of changes implemented by Service Provider, with the result expressed as a percentage. Changes will be reported in the Measurement Window that the Change ticket is closed, allowing sufficient time to determine if the Change was successful as defined in the Change Request. A low volume alternative calculation, set forth in Exhibit 3 , Service Level Matrix, Service Level Matrix, shall apply when the total volume of Service Requests falls within the volume (denominator) ranges specified in that Exhibit.
COLLECTION PROCESS	Change tickets will be logged in the Digital MSI Service Management 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. Change data will be uploaded to Digital MSI Service Management system on a daily basis. Digital MSI Service Management system will filter change tickets based on appropriate measurement criteria.
REPORTING TOOLS	As described in the process above, the following tools will be utilized: <ul style="list-style-type: none"> • SCP event monitoring system • Digital MSI Service Management System

	<ul style="list-style-type: none"> MSI CMDB Digital MSI Service Level Management Reporting system Service Management Manual
RAW DATA STORAGE (ARCHIVES)	Data used to calculate the SLA results for reporting will be stored in the Digital MSI Service Level Management Reporting system, which will be accessible to authorized users via inherent report drill-down functionality for a rolling 13 months. An additional 23 months of data is archived and can be made available via Digital MSI Service Level Management Reporting system upon request by DIR.
PERFORMANCE CATEGORY	Service Management
METRIC REPORTING	<input checked="" type="checkbox"/> Monthly <input type="checkbox"/> Quarterly <input type="checkbox"/> Semi Annual

A.5.2 Resolution Time – Sev 1 Managed Device Platinum Tier

SERVICE LEVEL NAME	EXHIBIT NUMBER	SECTION REFERENCE	START DATE
Resolution Time – Sev 1 Managed Device Platinum Tier	3-A	1.1.17	
SERVICE LEVEL TYPE	Critical Service Level		
CURRENTLY MEASURED	No		
SERVICE COMPONENT: AREA(S)	Security Monitoring & Device Management: Endpoint Management Services, IDS/IPS, HIPS, Firewalls, Web Application Firewalls, SIEM, MDS/MPS, SOC Services		
OBJECTIVE	To ensure acceptable levels of resolution to security device failures.		
METRIC DESCRIPTION	<p>The Service Level for “Resolution Time – Sev 1 Managed Device Platinum Tier” measures the percentage of time Service Provider resolves Severity Level 1 Incidents for Managed Devices Platinum Tier within the applicable timeframes.</p> <p>See the SMM for how to measure performance when the Severity Level of an Incident changes.</p>		
METRIC INCLUSIONS and DATA SOURCES	<p>The applicable resolution timeframes are listed below.</p> <p><u>Includes all Severity 1 Incidents for Managed Devices Platinum Tier:</u></p> <ul style="list-style-type: none"> ≤ 4 hours when an onsite visit is required ≤ 1 hour when the device can be restored remotely 		

METRIC EXCLUSIONS	Incidents related to Mainframe Batch Job ABENDs, backups (in any Service Component).
HOURS OF MEASUREMENT	24
DAYS OF MEASUREMENT	365(366)
MINIMUM SERVICE LEVEL	95.00%
EXPECTED SERVICE LEVEL	98.00%
ALGORITHM	<p>The Service Level calculation for “Resolution Time – Sev 1 Managed Device Platinum Tier” is the total number of Severity 1 Incidents for which the Resolution Time is less than 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 time 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> <p>A low volume alternative calculation, set forth in Exhibit 3, shall apply when the total volume of Incidents falls within the volume (denominator) ranges specified in that Exhibit.</p>
COLLECTION PROCESS	<p>Incident tickets will be logged in the Digital MSI Service Management 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 Digital MSI Service Level Management Reporting system on a daily basis. Digital MSI Service Level Management Reporting system will filter incident tickets based on appropriate measurement criteria.</p>

REPORTING TOOLS	<p>As described in the process above, the following tools will be utilized:</p> <ul style="list-style-type: none"> • SCP event monitoring system • Digital MSI Service Management System • MSI CMDB • Digital MSI Service Level Management Reporting system • Service Management Manual
RAW DATA STORAGE (ARCHIVES)	Data used to calculate the SLA results for reporting will be stored in the Digital MSI Service Level Management Reporting system, which will be accessible to authorized users via inherent report drill-down functionality for a rolling 13 months. An additional 23 months of data is archived and can be made available via Digital MSI Service Level Management Reporting system upon request by DIR.
PERFORMANCE CATEGORY	Service Management
METRIC REPORTING	<input checked="" type="checkbox"/> Monthly <input type="checkbox"/> Quarterly <input type="checkbox"/> Semi Annual

A.5.3 Resolution Time – Sev 1 Managed Device Gold Tier

SERVICE LEVEL NAME	EXHIBIT NUMBER	SECTION REFERENCE	START DATE
Resolution Time – Sev 1 Managed Device Gold Tier	3-A	1.1.18	
SERVICE LEVEL TYPE	Critical Service Level		
CURRENTLY MEASURED	No		
SERVICE COMPONENT: AREA(S)	Security Monitoring & Device Management: Endpoint Management Services, IDS/IPS, HIPS, Firewalls, Web Application Firewalls, SIEM, MDS/MPS, SOC Services		
OBJECTIVE	To ensure acceptable levels of resolution to security device failures.		
METRIC DESCRIPTION	The Service Level for “Resolution Time – Sev 1 Managed Device Gold Tier” measures the percentage of time the Service Provider resolves Severity Level 1 Incidents for Managed Devices Gold Tier within the applicable timeframes.		
METRIC INCLUSIONS and DATA SOURCES	<p>The applicable resolutions timeframes are listed below.</p> <p><u>Includes all Severity 1 Incidents for Managed Devices Gold Tier:</u></p> <ul style="list-style-type: none"> • ≤ 8 hours when an onsite visit is required • ≤ 4 hours when the device can be restored remotely 		
METRIC EXCLUSIONS	Incidents related to Mainframe Batch Job ABENDs, backups (in any Service Component).		

HOURS OF MEASUREMENT	24
DAYS OF MEASUREMENT	365(366)
MINIMUM SERVICE LEVEL	95.00%
EXPECTED SERVICE LEVEL	98.00%
ALGORITHM	<p>The Service Level calculation for “Resolution Time – Sev 1 Managed Device Gold Tier” is the total number of Severity 1 Incidents for which the Resolution Time is less than 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 time 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> <p>A low volume alternative calculation, set forth in Exhibit 3, shall apply when the total volume of Incidents falls within the volume (denominator) ranges specified in that Exhibit.</p>
COLLECTION PROCESS	<p>Incident tickets will be logged in the Digital MSI Service Management 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 Digital MSI Service Level Management Reporting system on a daily basis. Digital MSI Service Level Management Reporting system will filter incident tickets based on appropriate measurement criteria.</p>
REPORTING TOOLS	<p>As described in the process above, the following tools will be utilized:</p> <ul style="list-style-type: none"> • SCP event monitoring system • Digital MSI Service Management system • MSI CMDB • Digital MSI Service Level Management Reporting system • Service Management Manual

RAW DATA STORAGE (ARCHIVES)	Data used to calculate the SLA results for reporting will be stored in the Digital MSI Service Level Management Reporting system, which will be accessible to authorized users via inherent report drill-down functionality for a rolling 13 months. An additional 23 months of data is archived and can be made available via Digital MSI Service Level Management Reporting system upon request by DIR.
PERFORMANCE CATEGORY	Service Management
METRIC REPORTING	<input checked="" type="checkbox"/> Monthly <input type="checkbox"/> Quarterly <input type="checkbox"/> Semi Annual

A.5.4 Managed Device – Platinum Tier Availability

SERVICE LEVEL NAME	EXHIBIT NUMBER	SECTION REFERENCE	START DATE
Managed Device – Platinum Tier Availability	3-A	1.1.19	
SERVICE LEVEL TYPE	Critical Service Level		
CURRENTLY MEASURED	No		
SERVICE COMPONENT: AREA(S)	Security Monitoring & Device Management: Endpoint Management Services, IDS/IPS, HIPS, Firewalls, Web Access Firewalls, SIEM, MDS/MPS, SOC Services		
OBJECTIVE	To ensure acceptable levels of availability for Managed Devices		
METRIC DESCRIPTION	The Service Level for “Managed Device - Platinum Tier Availability” measures the percentage of time the Managed Device Platinum Tier is Available to the end-user during the applicable Measurement Window. If Downtime occurs for a Managed Device, the Outage is counted against the Managed Device, and the Managed Device is considered unavailable for purposes of this Service Level.		
METRIC INCLUSIONS and DATA SOURCES	Managed Devices are identified in the CMDB. Scheduled hours of operations and maintenance windows for each infrastructure element related to the Managed Device will be maintained in the SMM.		
METRIC EXCLUSIONS	Failures that do not result in any Managed Device incurring Downtime.		
HOURS OF MEASUREMENT	24		
DAYS OF MEASUREMENT	365(366)		
MINIMUM SERVICE LEVEL	99.99%		

EXPECTED SERVICE LEVEL	99.99%
ALGORITHM	The Service Level calculation for “Managed Device – Platinum Tier Availability” is the sum of Actual Uptime for all Platinum Managed Devices, divided by the sum of Critical Uptime for all such Platinum Managed Devices, with the result expressed as a percentage.
COLLECTION PROCESS	<p>If an outage event occurs it will be identified by the responsible Service Component Provider (SCP) event monitoring system or by a user initiated incident, and tracked to resolution via an incident ticket in the MSI Incident ticketing system.</p> <p>The MSS SCP will improve the Incident ticket quality, including unavailability records and accurate Start Time, via root cause analysis for Severity 1 and 2 Incidents, and the use of tools if such tool data is available.</p> <p>For reporting purposes, required data elements will be collected from each of the data sources. For example:</p> <ul style="list-style-type: none"> • Digital MSI Service Management System - incident ticket number, incident summary, incident resolution text, resolution time, impacted CI name(s), actual outage start time, actual outage stop time, and outage duration • MSI CMDB - server instances and related CIs supporting impacted application • Service Management Manual - maintenance schedules, hours of operation <p>Collected data will be sourced by the Digital MSI Service Level Management Reporting system application for purposes of aggregating, calculating, measuring and reporting SLA results. Manual input will be considered for purposes of supplementing collected data where necessary.</p>
REPORTING TOOLS	<p>As described in the process above, the following tools will be utilized:</p> <ul style="list-style-type: none"> • SCP event monitoring system • Digital MSI Service Management system • MSI CMDB • Digital MSI Service Level Management Reporting system • Service Management Manual
RAW DATA STORAGE (ARCHIVES)	Data used to calculate the SLA results for reporting will be stored in the Digital MSI Service Level Management Reporting system, which will be accessible to authorized users via inherent report drill-down functionality for a rolling 13 months. An additional 23 months of data is archived and can be made available via Digital MSI Service Level Management Reporting system upon request by DIR.
PERFORMANCE CATEGORY	Service Management

METRIC REPORTING	<input checked="" type="checkbox"/> Monthly <input type="checkbox"/> Quarterly <input type="checkbox"/> Semi Annual
-------------------------	---

A.5.5 Managed Device – Gold Tier Availability

SERVICE LEVEL NAME	EXHIBIT NUMBER	SECTION REFERENCE	START DATE
Managed Device – Gold Tier Availability	3-A	1.1.20	
SERVICE LEVEL TYPE	Critical Service Level		
CURRENTLY MEASURED	No		
SERVICE COMPONENT: AREA(S)	Security Monitoring & Device Management: Endpoint Management Services, IDS/IPS, HIPS, Firewalls, Web Access Firewalls, SIEM, MDS/MPS, SOC Services		
OBJECTIVE	To ensure acceptable levels of availability for Managed Devices		
METRIC DESCRIPTION	The Service Level for “Managed Device - Gold Tier Availability” measures the percentage of time the Managed Device Gold Tier is Available to the end-user during the applicable Measurement Window. If Downtime occurs for a Managed Device, the Outage is counted against the Managed Device, and the Managed Device is considered unavailable for purposes of this Service Level.		
METRIC INCLUSIONS and DATA SOURCES	Managed Devices are identified in the CMDB. Scheduled hours of operations and maintenance windows for each infrastructure element related to the Managed Device will be maintained in the SMM.		
METRIC EXCLUSIONS	Failures that do not result in any Managed Device incurring Downtime.		
HOURS OF MEASUREMENT	24		
DAYS OF MEASUREMENT	365(366)		
MINIMUM SERVICE LEVEL	99.00%		
EXPECTED SERVICE LEVEL	99.80%		
ALGORITHM	The Service Level calculation for “Managed Device – Gold Tier Availability” is the sum of Actual Uptime for all Gold Managed Devices, divided by the sum of Critical Uptime for all such Gold Managed Devices, with the result expressed as a percentage.		

<p>COLLECTION PROCESS</p>	<p>If an outage event occurs it will be identified by the responsible Service Component Provider (SCP) event monitoring system or by a user initiated incident, and tracked to resolution via an incident ticket in the MSI Incident ticketing system.</p> <p>The MSS SCP will improve the Incident ticket quality, including unavailability records and accurate Start Time, via root cause analysis for Severity 1 and 2 Incidents, and the use of tools if such tool data is available.</p> <p>For reporting purposes, required data elements will be collected from each of the data sources. For example:</p> <ul style="list-style-type: none"> • Digital MSI Service Management system - incident ticket number, incident summary, incident resolution text, resolution time, impacted CI name(s), actual outage start time, actual outage stop time, and outage duration • MSI CMDB - server instances and related CIs supporting impacted application • Service Management Manual - maintenance schedules, hours of operation <p>Collected data will be sourced by the Digital MSI Service Level Management Reporting system application for purposes of aggregating, calculating, measuring and reporting SLA results. Manual input will be considered for purposes of supplementing collected data where necessary.</p>
<p>REPORTING TOOLS</p>	<p>As described in the process above, the following tools will be utilized:</p> <ul style="list-style-type: none"> • SCP event monitoring system • Digital MSI Service Management system • MSI CMDB • Digital MSI Service Level Management Reporting system • Service Management Manual
<p>RAW DATA STORAGE (ARCHIVES)</p>	<p>Data used to calculate the SLA results for reporting will be stored in the Digital MSI Service Level Management Reporting system, which will be accessible to authorized users via inherent report drill-down functionality for a rolling 13 months. An additional 23 months of data is archived and can be made available via Digital MSI Service Level Management Reporting system upon request by DIR.</p>
<p>PERFORMANCE CATEGORY</p>	<p>Service Management</p>
<p>METRIC REPORTING</p>	<p><input checked="" type="checkbox"/> Monthly <input type="checkbox"/> Quarterly <input type="checkbox"/> Semi Annual</p>

A.5.6 Patch Compliance – Managed Device

SERVICE LEVEL NAME	EXHIBIT NUMBER	SECTION REFERENCE	START DATE
Patch Compliance – Managed Device	3-A	1.1.21	
SERVICE LEVEL TYPE	Critical Service Level		
CURRENTLY MEASURED	No		
SERVICE COMPONENT: AREA(S)	Security Monitoring & Device Management: Endpoint Management Services, IDS/IPS, HIPS, Firewalls, Web Application Firewalls, SIEM, MDS/MPS, SOC Services		
OBJECTIVE	To ensure timely notification and compliance with all security and software patches		
METRIC DESCRIPTION	<p>Measure the percentage of applicable patches that are scheduled for implementation via an opened RITM ticket within three (3) Business Days of the patch availability. The Service Level will be measured via a RITM tracking the time from patch availability to routing for Customer approval. Upon customer approval, a Change Request will be automatically generated for patch implementation.</p> <p>This Service Level will take effect on 9/1/18.</p>		
METRIC INCLUSIONS and DATA SOURCES	Managed Devices are identified in the CMDB. Scheduled hours of operations and maintenance windows for each infrastructure element related to the Managed Device will be maintained in the SMM.		
METRIC EXCLUSIONS	Patches not applicable to Customer as defined in configurations and settings.		
HOURS OF MEASUREMENT	24		
DAYS OF MEASUREMENT	365(366)		
MINIMUM SERVICE LEVEL	95.00%		
EXPECTED SERVICE LEVEL	98.00%		

<p>ALGORITHM</p>	<p>The Service Level calculation is the total number of Patch Compliance RITMs that are sent to the Customer for approval within three (3) Business Days from Patch Availability date, divided by the total number of resolved RITMs plus the total number of open RITMs that have exceeded the committed timeframes, with the result expressed as a percentage.</p> <p>For purposes of clarity, note the following:</p> <p>(a) if a RITM 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 RITM 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 RITM 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 resolution 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.</p> <p>A low volume alternative calculation, set forth in Exhibit 3, Service Level Matrix, shall apply when the total volume of Service Requests falls within the volume (denominator) ranges specified in that Exhibit.</p>
<p>COLLECTION PROCESS</p>	<p>RITM tickets will be logged in the Digital MSI Service Management system. RITMs 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.</p> <p>Change data will be uploaded to MSI systems on a daily basis. MSI systems will filter change tickets based on appropriate measurement criteria.</p>
<p>REPORTING TOOLS</p>	<p>As described in the process above, the following tools will be utilized:</p> <ul style="list-style-type: none"> • SCP event monitoring system • Digital MSI Service Management System • Digital MSI Service Level Management Reporting system • Service Management Manual
<p>RAW DATA STORAGE (ARCHIVES)</p>	<p>Data used to calculate the SLA results for reporting will be stored in the Digital MSI Service Level Management Reporting system, which will be accessible to authorized users via inherent report drill-down functionality for a rolling 13 months. An additional 23 months of data is archived and can be made available via Digital MSI Service Level Management Reporting system upon request by DIR.</p>

PERFORMANCE CATEGORY	Service Management
METRIC REPORTING	<input checked="" type="checkbox"/> Monthly <input type="checkbox"/> Quarterly <input type="checkbox"/> Semi Annual

A.5.7 Managed Device Outage Notification

SERVICE LEVEL NAME	EXHIBIT NUMBER	SECTION REFERENCE	START DATE
Managed Device Outage Notification	3-A	1.1.23	
SERVICE LEVEL TYPE	Critical Service Level		
CURRENTLY MEASURED	No		
SERVICE COMPONENT: AREA(S)	Security Monitoring & Device Management: Endpoint Management Services, IDS/IPS, HIPS, Firewalls, Web Application Firewalls, SIEM, MDS/MPS, SOC Services		
OBJECTIVE	To ensure timely notification of outage on managed devices		
METRIC DESCRIPTION	The Service Level for Managed Device Outage Notification measures the percentage of incidents where the Customer is notified within fifteen (15) minutes of a device failure, measured from the time of the device failure to the time the Customer is notified of the failure.		
METRIC INCLUSIONS and DATA SOURCES	Managed Devices are identified in the CMDB. Scheduled hours of operations and maintenance windows for each infrastructure element related to the Managed Device will be maintained in the SMM.		
METRIC EXCLUSIONS	Failures that do not result in any Managed Device incurring Downtime.		
HOURS OF MEASUREMENT	24		
DAYS OF MEASUREMENT	365(366)		
MINIMUM SERVICE LEVEL	95.00%		
EXPECTED SERVICE LEVEL	98.00%		

<p>ALGORITHM</p>	<p>The Service Level calculation for “Managed Device Outage Notification” is the total number of Security Monitoring & Device Management device failure Incidents that are resolved during the applicable Measurement Window, for which Service Provider provided the applicable Authorized User the required notice, divided by the total number of Security Monitoring & Device Management device failure Incidents that are resolved during the applicable Measurement Window, with the result expressed as a percentage.</p> <p>A low volume alternative calculation, set forth in Exhibit <u>3</u>, Service Level Matrix, Service Level Matrix, shall apply when the total volume of Service Requests falls within the volume (denominator) ranges specified in that Exhibit.</p>
<p>COLLECTION PROCESS</p>	<p>Incident tickets will be logged in the Digital MSI Service Management 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. The Digital MSI Service Management Incident ticket will note the time of the device failure and time the Service Provider provided the applicable Authorized User the required notice.</p> <p>Incident data will be uploaded to Digital MSI Service Level Management Reporting system on a daily basis. Digital MSI Service Level Management Reporting system will filter incident tickets based on appropriate measurement criteria.</p>
<p>REPORTING TOOLS</p>	<p>As described in the process above, the following tools will be utilized:</p> <ul style="list-style-type: none"> • SCP event monitoring system • Digital MSI Service Management System • MSI CMDB • Digital MSI Service Level Management Reporting system • Service Management Manual
<p>RAW DATA STORAGE (ARCHIVES)</p>	<p>Data used to calculate the SLA results for reporting will be stored in the Digital MSI Service Level Management Reporting system, which will be accessible to authorized users via inherent report drill-down functionality for a rolling 13 months. An additional 23 months of data is archived and can be made available via Digital MSI Service Level Management Reporting system upon request by DIR.</p>
<p>PERFORMANCE CATEGORY</p>	<p>Service Management</p>
<p>METRIC REPORTING</p>	<p><input checked="" type="checkbox"/> Monthly <input type="checkbox"/> Quarterly <input type="checkbox"/> Semi Annual</p>

A.6 Service Area Service Levels – Incident Response

This Section A.6 shall apply to the Incident Response Service Component.

This Section sets forth qualitative descriptions of the Critical Service Levels for the Incident Response Service Component. The numerical Minimum Service Levels, Expected Service Levels and commencement of obligations associated with such Critical Service Levels are set forth in **Attachment 3-A**, CSLs – Incident Response tab.

SERVICE LEVEL NAME	EXHIBIT NUMBER	SECTION REFERENCE	START DATE

A.6.1 Time to Deliver Staff (qualified and screened) Remotely

SERVICE LEVEL NAME	EXHIBIT NUMBER	SECTION REFERENCE	START DATE
Time to Deliver Staff (qualified and screened) Remotely	3-A	1.1.26	
SERVICE LEVEL TYPE	Critical Service Level		
CURRENTLY MEASURED	No		
SERVICE COMPONENT: AREA(S)	Incident Response: Incident Management, Digital Forensics		
OBJECTIVE	To ensure staff needed to perform Services are provided to Customer promptly		
METRIC DESCRIPTION	Measure of the percentage of Customer requests for staff fulfilled within eight (8) hours, calculated from the time the Customer approves the Service Provider’s staff proposal to the time the Service Provider’s qualified and background check compliant staff are actively engaged with the Customer by phone or other remote electronic means		
METRIC INCLUSIONS and DATA SOURCES	Qualified and screened requirements for staff will be maintained in the SMM. Scheduled hours of operations related to the Services will be maintained in the SMM.		
METRIC EXCLUSIONS	N/A		
HOURS OF MEASUREMENT	24		
DAYS OF MEASUREMENT	365(366)		
MINIMUM SERVICE LEVEL	95.00%		
EXPECTED SERVICE LEVEL	98.00%		

<p>ALGORITHM</p>	<p>The Service Level calculation for “Time to Deliver Staff Remotely” is the total number of requests that are successfully completed within the committed timeframes, divided by the total number of requests completed with the result expressed as a percentage.</p> <p>For purposes of clarity, note the following:</p> <p>(a) if a Project 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 Service Request 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 Project 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.</p> <p>A low volume alternative calculation, set forth in Exhibit <u>3</u>, Service Level Matrix, Service Level Matrix, shall apply when the total volume of Projects falls within the volume (denominator) ranges specified in that Exhibit.</p>
<p>COLLECTION PROCESS</p>	<p>Requests to deliver staff remotely will be logged and tracked in the Digital MSI Service Management System.</p> <p>Requests will be categorized and assigned to resolver teams who will work to resolve the request and progress the ticket through the request management lifecycle.</p> <p>Service Request data will be uploaded to Digital MSI Service Level Management Reporting system on a daily basis. Digital MSI Service Level Management Reporting system will filter tickets based on appropriate measurement criteria.</p>
<p>REPORTING TOOLS</p>	<p>As described in the process above, the following tools will be utilized:</p> <ul style="list-style-type: none"> • Digital MSI Service Management System • Digital MSI Service Level Management Reporting system • Service Management Manual
<p>RAW DATA STORAGE (ARCHIVES)</p>	<p>Data used to calculate the SLA results for reporting will be stored in the Digital MSI Service Level Management Reporting system database, which will be accessible to authorized users via inherent report drill-down functionality for a rolling 13 months. An additional 23 months of data is archived and can be made available via Digital MSI Service Level Management Reporting system upon request by DIR.</p>
<p>PERFORMANCE CATEGORY</p>	<p>Service Management</p>

METRIC REPORTING	<input checked="" type="checkbox"/> Monthly <input type="checkbox"/> Quarterly <input type="checkbox"/> Semi Annual
-------------------------	---

A.6.2 Time to Deliver Staff (qualified and screened) Onsite

SERVICE LEVEL NAME	EXHIBIT NUMBER	SECTION REFERENCE	START DATE
Time to Deliver Staff (qualified and screened) Onsite	3-A	1.1.27	
SERVICE LEVEL TYPE	Critical Service Level		
CURRENTLY MEASURED	No		
SERVICE COMPONENT: AREA(S)	Incident Response: Incident Management, Digital Forensics		
OBJECTIVE	To ensure staff needed to perform Services are provided to Customer promptly		
METRIC DESCRIPTION	Measure of the percentage of Customer requests for staff fulfilled within forty-eight (48) hours, calculated from the time the Customer approves the Service Provider's staff proposal to the time the Service Provider's qualified and background check compliant staff are actively engaged with the Customer at the Customer's site		
METRIC INCLUSIONS and DATA SOURCES	Qualified and screened requirements for staff will be maintained in the SMM. Scheduled hours of operations related to the Services will be maintained in the SMM.		
METRIC EXCLUSIONS	N/A		
HOURS OF MEASUREMENT	24		
DAYS OF MEASUREMENT	365(366)		
MINIMUM SERVICE LEVEL	95.00%		
EXPECTED SERVICE LEVEL	98.00%		

<p>ALGORITHM</p>	<p>The Service Level calculation for “Time to Deliver Staff Onsite” is the total number of requests that are successfully completed within the committed timeframes, divided by the total number of requests completed with the result expressed as a percentage.</p> <p>For purposes of clarity, note the following:</p> <p>(a) if a Project 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 Service Request 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 Project 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.</p> <p>A low volume alternative calculation, set forth in Exhibit <u>3</u>, Service Level Matrix, Service Level Matrix, shall apply when the total volume of Projects falls within the volume (denominator) ranges specified in that Exhibit.</p>
<p>COLLECTION PROCESS</p>	<p>Requests will be categorized and assigned to resolver teams who will work to resolve the request and progress the ticket through the request management lifecycle. Service Request data will be uploaded to Digital MSI Service Level Management Reporting system on a daily basis. Digital MSI Service Level Management Reporting system will filter tickets based on appropriate measurement criteria.</p>
<p>REPORTING TOOLS</p>	<p>As described in the process above, the following tools will be utilized:</p> <ul style="list-style-type: none"> • Digital MSI Service Management System • Digital MSI Service Level Management Reporting system • Service Management Manual
<p>RAW DATA STORAGE (ARCHIVES)</p>	<p>Data used to calculate the SLA results for reporting will be stored in the Digital MSI Service Level Management Reporting system, which will be accessible to authorized users via inherent report drill-down functionality for a rolling 13 months. An additional 23 months of data is archived and can be made available via Digital MSI Service Level Management Reporting system upon request by DIR.</p>
<p>PERFORMANCE CATEGORY</p>	<p>Service Management</p>
<p>METRIC REPORTING</p>	<p><input checked="" type="checkbox"/> Monthly <input type="checkbox"/> Quarterly <input type="checkbox"/> Semi Annual</p>

A.7 Service Area Service Levels – Risk & Compliance

This Section A.7 shall apply to the Risk and Compliance Service Component.

This Section sets forth qualitative descriptions of the Critical Service Levels for the Risk & Compliance Service Component. The numerical Minimum Service Levels, Expected Service Levels and commencement of obligations associated with such Critical Service Levels are set forth in **Attachment 3-A**, CSLs – Risk & Compliance tab.

A.7.1 Notification of Critical or High Risk Vulnerabilities to Customer

SERVICE LEVEL NAME	EXHIBIT NUMBER	SECTION REFERENCE	START DATE
Notification of Critical or High Risk Vulnerabilities to Customer	3-A	1.1.28	
SERVICE LEVEL TYPE	Critical Service Level		
CURRENTLY MEASURED	No		
SERVICE COMPONENT: AREA(S)	Risk & Compliance: Penetration Testing, Risk Assessment, Cloud Compliance, Vulnerability Scanning, Web Application Scanning		
OBJECTIVE	To ensure timely notification to and delivery of any/all critical and/or high risk vulnerabilities as identified to the Customer		
METRIC DESCRIPTION	Measure of the percentage of high risk or critical vulnerabilities where the Customer is notified within four (4) hours of the vulnerability verification, calculated from the time Service Provider identifies the vulnerability to the time the Customer is notified.		
METRIC INCLUSIONS and DATA SOURCES	The item being tested, assessed, or scanned will be identified in the Customer’s request. Scheduled hours of operations and maintenance windows for the item being tested, assessed, or scanned will be maintained in the SPP.		
METRIC EXCLUSIONS	Incidents resulting in any Managed Device incurring Downtime.		
HOURS OF MEASUREMENT	24		
DAYS OF MEASUREMENT	365(366)		
MINIMUM SERVICE LEVEL	95.00%		
EXPECTED SERVICE LEVEL	98.00%		

ALGORITHM	<p>The Service Level calculation for “Notification of Critical or High Risk Vulnerabilities to Customer” is the total number of Risk & Compliance vulnerability Service Requests that are completed during the applicable Measurement Window, for which Service Provider provided the applicable Authorized User the required notice, divided by the total number of Risk & Compliance vulnerability Service Requests that are completed during the applicable Measurement Window, with the result expressed as a percentage.</p> <p>A low volume alternative calculation, set forth in Exhibit <u>3</u>, Service Level Matrix, Service Level Matrix, shall apply when the total volume of Service Requests falls within the volume (denominator) ranges specified in that Exhibit.</p>
COLLECTION PROCESS	<p>Service Requests tickets will be logged in the Digital MSI Service Management system. Service Requests will be categorized and assigned to resolver teams who will work to complete the Service Requests and progress the ticket through the request management lifecycle.</p> <p>Service Requests data will be uploaded to Digital MSI Service Level Management Reporting system on a daily basis. Digital MSI Service Level Management Reporting system will filter incident tickets based on appropriate measurement criteria.</p>
REPORTING TOOLS	<p>As described in the process above, the following tools will be utilized:</p> <ul style="list-style-type: none"> • SCP tools • Digital MSI Service Management System • Digital MSI Service Level Management Reporting system • Service Management Manual
RAW DATA STORAGE (ARCHIVES)	<p>Data used to calculate the SLA results for reporting will be stored in the Digital MSI Service Level Management Reporting system, which will be accessible to authorized users via inherent report drill-down functionality for a rolling 13 months. An additional 23 months of data is archived and can be made available via Digital MSI Service Level Management Reporting system upon request by DIR.</p>
PERFORMANCE CATEGORY	Service Management
METRIC REPORTING	<input checked="" type="checkbox"/> Monthly <input type="checkbox"/> Quarterly <input type="checkbox"/> Semi Annual

B.0 KEY MEASUREMENTS – MANAGED SECURITY

This Section sets forth qualitative descriptions of the Key Measurements for the Service Component(s) indicated. The numerical Minimum Service Levels, Expected Service Levels and commencement of obligations associated with such Key Measurements are set forth in **Attachment 3-A**, Key Measures-MSS tab.

B.1 Root Cause Analysis Delivery

SERVICE LEVEL NAME	EXHIBIT NUMBER	SECTION REFERENCE	START DATE
Root Cause Analysis Delivery – Security Monitoring & Device Management Root Cause Analysis Delivery – Incident Response Root Cause Analysis Delivery – Risk and Compliance	3-A		0
SERVICE LEVEL TYPE	Key Measurement		
CURRENTLY MEASURED	Yes		
SERVICE COMPONENT(S)	Security Monitoring & Device Management, Incident Response, Risk and Compliance		
METRIC DESCRIPTION	The Service Level “Root Cause Analysis Delivery” measures the percentage of time Service Provider delivers to Customer, via email, a Root Cause Analyses within (i) ten (10) Business Days from service restoration (for Severity 1), (ii) ten (10) Business Days from request, (iii) ten (10) Business Days from Service Level Improvement Plan initiation, or (iv) otherwise as agreed upon by DIR.		
METRIC INCLUSIONS and DATA SOURCES	<p>The RCA is documented and tracked within the Problem Management process, and upon completion, is presented by the Service Provider Problem Management Team to the affected DCS Customer and DIR for review and approval.</p> <p>Service Provider will provide Root Cause Analyses on the most business-critical events, as determined by the ‘DCS Critical List’ maintained in the SMM, and as reasonably requested by DIR or DCS Customers for all other Incidents.</p>		
METRIC EXCLUSIONS	N/A		
HOURS OF MEASUREMENT	8:00 AM – 5:00 PM		
DAYS OF MEASUREMENT	Business Days		
MINIMUM SERVICE LEVEL	96.00%		
EXPECTED SERVICE LEVEL	98.00%		

ALGORITHM	<p>The Service Level calculation for “Root Cause Analysis Delivery” is the total number of Root Cause Analyses that are delivered to Customer within the required timeframe, divided by the total number of Root Cause Analyses delivered to Customer during the applicable Measurement Window, with the result expressed as a percentage.</p> <p>If the Service Provider misses one (1) delivery of an RCA, then the performance for this Service Level shall either be calculated using the standard algorithm, or deemed to equal the Minimum Service Level target, whichever is higher.</p>
COLLECTION PROCESS	<p>Problem investigations (requests for Root Cause Analysis) will be logged and tracked in the Digital MSI Service Management System. Problems will be categorized and assigned to teams who will analyze the request and perform and document the root cause analysis. The problem ticket will be progressed through the problem management lifecycle.</p> <p>Problem data will be uploaded to Digital MSI Service Level Management Reporting system on a daily basis. Digital MSI Service Level Management Reporting system will filter Problem tickets based on appropriate measurement criteria.</p>
REPORTING TOOLS	<ul style="list-style-type: none"> • Digital MSI Service Management System • Digital MSI Service Level Management Reporting system
RAW DATA STORAGE (ARCHIVES)	<p>Data used to calculate the SLA results for reporting will be stored in the Digital MSI Service Level Management Reporting system, which will be accessible to authorized users via inherent report drill-down functionality for a rolling 13 months. An additional 23 months of data is archived and can be made available via Digital MSI Service Level Management Reporting system upon request by DIR.</p>
PERFORMANCE CATEGORY	Incident and Problem
METRIC REPORTING	<input checked="" type="checkbox"/> Monthly <input type="checkbox"/> Quarterly <input type="checkbox"/> Semi Annual

B.2 Corrective Actions

SERVICE LEVEL NAME	EXHIBIT NUMBER	SECTION REFERENCE	START DATE
Corrective Actions – Security Monitoring & Device Management Corrective Actions – Incident Response Corrective Actions – Risk and Compliance	3-A		0
SERVICE LEVEL TYPE	Key Measurement		

CURRENTLY MEASURED	Yes
SERVICE COMPONENT(S)	Security Monitoring & Device Management, Incident Response, Risk and Compliance
METRIC DESCRIPTION	The Service Level “Corrective Actions” measures the percentage of time Service Provider completes corrective actions within the committed timeframes.
METRIC INCLUSIONS and DATA SOURCES AND DATA SOURCE	Corrective Actions associated with all Managed Security Service Component Problem tickets.
METRIC EXCLUSIONS	Corrective Actions internal to Service Provider other than those for Service Level Improvement Plans.
HOURS OF MEASUREMENT	N/A
DAYS OF MEASUREMENT	N/A
MINIMUM SERVICE LEVEL	95.00%
EXPECTED SERVICE LEVEL	98.00%
ALGORITHM	<p>The Service Level calculation for “Corrective Actions” is the total number of Corrective Actions that are completed within the required timeframe, divided by the total number of Corrective Actions completed plus the total number of Corrective Actions that have passed the committed timeframe, with the result expressed as a percentage.</p> <p>For purposes of clarity, note the following:</p> <p>(a) if a Corrective Action 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 Corrective Action is actually closed in the current Measurement Window, in which case it is included in the current Measurement Window’s calculation).</p> <p>(b) an open Corrective Action that has exceeded the committed timeframe is also carried forward into subsequent Measurement Windows as a breach until closed; if it is closed 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 committed timeframes in each subsequent Measurement Window’s calculation until closed.</p>

COLLECTION PROCESS	<p>Corrective Actions will be logged and tracked in the Digital MSI Service Management System. Corrective Actions will be assigned to teams who will implement the Corrective Actions. The Corrective Actions will be progressed through the problem management lifecycle.</p> <p>Problem data, including Corrective Actions, will be uploaded to Digital MSI Service Level Management Reporting system on a daily basis. Digital MSI Service Level Management Reporting system will filter Problem tickets based on appropriate measurement criteria.</p>
REPORTING TOOLS	<ul style="list-style-type: none"> • Digital MSI Service Management System • Digital MSI Service Level Management Reporting system
RAW DATA STORAGE (ARCHIVES)	Data used to calculate the SLA results for reporting will be stored in the Digital MSI Service Level Management Reporting system database, which will be accessible to authorized users via inherent report drill-down functionality for a rolling 13 months. An additional 23 months of data is archived and can be made available via Digital MSI Service Level Management Reporting system upon request by DIR.
PERFORMANCE CATEGORY	Incident and Problem
METRIC REPORTING	<input checked="" type="checkbox"/> Monthly <input type="checkbox"/> Quarterly <input type="checkbox"/> Semi Annual

B.3 Resolution Time – Severity Level 1, 2, 3 and 4

SERVICE LEVEL NAME	EXHIBIT NUMBER	SECTION REFERENCE	START DATE
<i>Resolution Time – Sev 1, 2, 3 and 4</i>	3-A		0
SERVICE LEVEL TYPE	Key Measurement		
CURRENTLY MEASURED	Yes		
SERVICE COMPONENT(S)	Security Monitoring & Device Management, Risk and Compliance Incident Response		
METRIC DESCRIPTION	<p>The Service Level for “Resolution Time – Sev 1, 2, 3 and 4” measures the percentage of time Service Provider Resolves Incidents within the applicable timeframes.</p> <p>See the SMM for how to measure performance when the Severity Level of an Incident changes.</p>		

<p>METRIC INCLUSIONS and DATA SOURCES</p>	<p>The applicable resolution timeframes are listed below. Includes all Severity 1, 2, 3 and 4 Incidents for Security Monitoring & Device Management and Incident Response Service Components except as excluded below.</p> <p><u>Severity 1</u></p> <ul style="list-style-type: none"> • ≤ 4 hours <p><u>Severity 2</u></p> <ul style="list-style-type: none"> • ≤ 6 hours <p><u>Severity 3</u></p> <ul style="list-style-type: none"> • The Incident shall be Resolved within 540 minutes (i.e. 9 hours or 1 Business Day) where such minutes shall be measured only between 8:00 AM and 5:00 PM inclusive on Business Days. <p><u>Severity 4</u></p> <ul style="list-style-type: none"> • The Incident shall be Resolved within 2160 minutes (i.e. 36 hours or 4 Business Days) where such minutes shall be measured only between 8:00 AM and 5:00 PM inclusive on Business Days.
<p>METRIC EXCLUSIONS</p>	<p>Severity 1 Incidents for Security Monitoring & Device Management Platinum Tier (measured in A.5.2) and Gold Tier (measured in A.5.3). Incidents related to Mainframe Batch Job ABENDS, backups (in any Service Component).</p> <p>Events determined to be outside the control of the Service Provider, including but not limited to DCS outages, Customer work on systems or applications, or Force Majeure Events.</p>
<p>HOURS OF MEASUREMENT</p>	<p>Sev 1 and Sev 2: 24 Sev 3 and Sev 4: 8:00 AM – 5:00 PM</p>
<p>DAYS OF MEASUREMENT</p>	<p>Sev 1 and Sev 2: 365(366) Sev 3 and Sev 4: Business Days</p>
<p>MINIMUM SERVICE LEVEL</p>	<p>95.00%</p>
<p>EXPECTED SERVICE LEVEL</p>	<p>98.00%</p>
<p>ALGORITHM</p>	<p>The Service Level calculation for “Resolution Time – Sev 1, 2, 3 and 4” is the total number of Incidents for which the Resolution Time is less than 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: (a) if an Incident is opened within the current Measurement Window, but its relevant resolution timeframe extends beyond the end of the</p>

	<p>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> <p>A low volume alternative calculation, set forth in Exhibit 3, Service Level Matrix, shall apply when the total volume of Incidents falls within the volume (denominator) ranges specified in that Exhibit.</p>
COLLECTION PROCESS	<p>Incident tickets will be logged in the Digital MSI Service Management 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 Digital MSI Service Level Management Reporting system on a daily basis. Digital MSI Service Level Management Reporting system will filter incident tickets based on appropriate measurement criteria.</p>
REPORTING TOOLS	<ul style="list-style-type: none"> • Digital MSI Service Management System • Digital MSI Service Level Management Reporting system
RAW DATA STORAGE (ARCHIVES)	<p>Data used to calculate the SLA results for reporting will be stored in the Digital MSI Service Level Management Reporting system, which will be accessible to authorized users via inherent report drill-down functionality for a rolling 13 months. An additional 23 months of data is archived and can be made available via Digital MSI Service Level Management Reporting system upon request by DIR.</p>
PERFORMANCE CATEGORY	Incident and Problem
METRIC REPORTING	<input checked="" type="checkbox"/> Monthly <input type="checkbox"/> Quarterly <input type="checkbox"/> Semi Annual

B.4 Service Request Fulfillment

SERVICE LEVEL NAME	EXHIBIT NUMBER	SECTION REFERENCE	START DATE
Service Request Fulfillment – Security Monitoring & Device Management	3-A		0

Service Request Fulfillment – Incident Response			
Service Request Fulfillment – Risk and Compliance			
SERVICE LEVEL TYPE	Key Measurement		
CURRENTLY MEASURED	Yes		
SERVICE COMPONENT(S)	Security Monitoring & Device Management, Incident Response, Risk and Compliance		
METRIC DESCRIPTION	<p>The Service Level for “Service Request Fulfillment” measures the percentage of time Service Provider successfully completes “Service Requests” (which are defined as requests that do not require solution proposal development; examples of such requests include provisioning ID access, password resets, Service Catalog requests, etc.).</p> <p>Specific target timeframes are maintained in the SMM.</p>		
METRIC INCLUSIONS and DATA SOURCES	Service Requests shall be an agreed upon set of service requests as specified in the SMM.		
METRIC EXCLUSIONS	Service Requests related to data recoveries.		
HOURS OF MEASUREMENT	As maintained in SMM		
DAYS OF MEASUREMENT	As maintained in SMM		
MINIMUM SERVICE LEVEL	90.00%		
EXPECTED SERVICE LEVEL	95.00%		
ALGORITHM	<p>The Service Level calculation for “Service Request” is the total number of Service Requests that are resolved within the committed timeframes, divided by the total number of resolved Service Requests plus the total number of open Service Requests that have exceeded the committed timeframes, with the result expressed as a percentage.</p> <p>For purposes of clarity, note the following:</p> <p>(a) if a Service 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 Service Request 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 Service Request 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 resolution 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.</p>		

	A low volume alternative calculation, set forth in Exhibit 3 , Service Level Matrix, Service Level Matrix, shall apply when the total volume of Service Requests falls within the volume (denominator) ranges specified in that Exhibit.
COLLECTION PROCESS	<p>Service Requests that do not require solution proposal development will be logged and tracked in the Digital MSI Service Management System. Service Requests will be categorized and assigned to resolver teams who will work to fulfill the Service Request and progress the ticket through the service request management lifecycle.</p> <p>Service Request data will be uploaded to Digital MSI Service Level Management Reporting system on a daily basis. Digital MSI Service Level Management Reporting system will filter service request tickets based on appropriate measurement criteria.</p>
REPORTING TOOLS	<ul style="list-style-type: none"> • Digital MSI Service Management System • Digital MSI Service Level Management Reporting system
RAW DATA STORAGE (ARCHIVES)	Data used to calculate the SLA results for reporting will be stored in the Digital MSI Service Level Management Reporting , which will be accessible to authorized users via inherent report drill-down functionality for a rolling 13 months. An additional 23 months of data is archived and can be made available via Digital MSI Service Level Management Reporting system upon request by DIR.
PERFORMANCE CATEGORY	Cross Functional
METRIC REPORTING	<input checked="" type="checkbox"/> Monthly <input type="checkbox"/> Quarterly <input type="checkbox"/> Semi Annual

B.5 Change Management Effectiveness

SERVICE LEVEL NAME	EXHIBIT NUMBER	SECTION REFERENCE	START DATE
Change Management Effectiveness – Security Monitoring & Device Management Change Management Effectiveness – Incident Response Change Management Effectiveness – Risk and Compliance	3-A		0
SERVICE LEVEL TYPE	Key Measurement		
CURRENTLY MEASURED	Yes, 12+ months of data available		
SERVICE COMPONENT(S)	Security Monitoring & Device Management, Incident Response, Risk and Compliance		

METRIC DESCRIPTION	The Service Level for “Change Management Effectiveness” measures the percentage of time Service Provider successfully implements Changes to the Services.
METRIC INCLUSIONS and DATA SOURCES	Includes all Managed Security Service Component Changes. Changes are not successfully implemented if they: (i) do not comply with the Change Management procedures (including the Change Control Process), the SMM and, except as specified in clause (ii) to this sentence, any associated project plan, (ii) cause either a Severity 1 Incident or Severity 2 Incident, (iv) exceeded the change window, (v) are backed out, or (vi) partial success of change is backed out or unsuccessful.
METRIC EXCLUSIONS	Change Request tickets to implement Filters/Signatures (measured in A.5.1) and/or Patches (measured in A.5.6).
HOURS OF MEASUREMENT	N/A
DAYS OF MEASUREMENT	N/A
MINIMUM SERVICE LEVEL	93.00%
EXPECTED SERVICE LEVEL	96.00%
ALGORITHM	<p>The Service Level calculation for “Change Management Effectiveness” is the number of changes that are successfully implemented by Service Provider divided by the number of changes implemented by Service Provider, with the result expressed as a percentage. Changes will be reported in the Measurement Window that the Change ticket is closed, allowing sufficient time to determine if the Change was successful as defined in the Change Request.</p> <p>A low volume alternative calculation, set forth in Exhibit 3, Service Level Matrix, Service Level Matrix, shall apply when the total volume of Service Requests falls within the volume (denominator) ranges specified in that Exhibit.</p>
COLLECTION PROCESS	<p>Change tickets will be logged in the Digital MSI Service Management 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.</p> <p>Change data will be uploaded to Digital MSI Service Level Management Reporting system on a daily basis. Digital MSI Service Level Management Reporting system will filter change tickets based on appropriate measurement criteria.</p>
REPORTING TOOLS	<ul style="list-style-type: none"> • Digital MSI Service Management System • Digital MSI Service Level Management Reporting system

RAW DATA STORAGE (ARCHIVES)	Data used to calculate the SLA results for reporting will be stored in the Digital MSI Service Level Management Reporting system, which will be accessible to authorized users via inherent report drill-down functionality for a rolling 13 months. An additional 23 months of data is archived and can be made available via the Digital MSI Service Level Management Reporting System upon request by DIR.
PERFORMANCE CATEGORY	Cross Functional
METRIC REPORTING	<input checked="" type="checkbox"/> Monthly <input type="checkbox"/> Quarterly <input type="checkbox"/> Semi Annual