

IRA J. ROSENTHAL
Chief Information Office &
Registrar of Voters
ijrosenthal@solanocounty.com
(707) 784-2703

Ramiro Carrasco
Assistant Director
rcarrasco@solanocounty.com
(707) 784-3035

DEPARTMENT OF INFORMATION TECHNOLOGY



**SOLANO
COUNTY**

675 Texas Street, Suite 3700
Fairfield, CA 94533-6342
Phone (707) 784-3000
Fax (707) 784-4883

www.solanocounty.com

Date: December 12, 2018

To: Solano County Board of Supervisors

cc: Birgitta Corsello
Jeanette Neiger
Michelle Heppner

From: Ira J Rosenthal

A handwritten signature in blue ink, appearing to read "Ira J Rosenthal", written over a light blue rectangular background.

Subject: Change to contract and staff report regarding Amendment 10 of the IT Services Agreement (ITSA) with Avenu Insights & Analytics, Inc.

Attached to this memo are changes to the staff report and ITSA that appear on the Board's agenda for December 11, 2018. The attached staff report shows redlined changes from the published version of the report. In addition, Exhibit A-1 and Exhibit A-2 of ITSA Amendment 10 (pages 3 and 4) will be replaced with those attached.

Our current ITSA is based on a fixed scope of work and staffing level. The contract includes a mechanism for adding work orders as needed to cover additional work requirements, and prior Board action has given the CIO authority to approve them.

The staff report submitted for the December 11th meeting and the accompanying contract were developed based on combining the current baseline scope of work with active work orders as a way to simplify administration of the contract.

As the department worked through operationalizing this proposed concept we discovered that we would lose contract and financial flexibility in excess of what we would gain administratively through simplification.

The revised documents revert to the current baseline scope and assume a continuation of the current practice of adjusting for new or additional workload through the use of work orders.

Prior Board action gave the CIO authority to approve work orders up to 10% of the contract amount. The revised staff report is requesting that this authority be increased to 15% so that this contract vehicle can be used for technical staffing of the SCIPS replacement project.

These changes will have no overall impact on budget appropriations for IT contract services.

Item 24

..title

Approve an amendment to the Information Technology Service Agreement (ITSA) with Avenu Insights & Analytics Inc. for \$~~5,350,6966,190,686~~ for the term of January 1, 2019 through December 31, 2019; Authorize the Chief Information Officer (CIO) to execute the agreement and to negotiate and execute change orders with Avenu, not to exceed 1540% of the contract amount and within departmental appropriations for IT contract services

..body

Published Notice Required? Yes ☐ No ☒
Public Hearing Required? Yes ☐ No ☒

DEPARTMENTAL RECOMMENDATION:

The Department of Information Technology recommends that the Board:

- 1) Approve an amendment to the Information Technology Service Agreement (ITSA) with Avenu Insights & Analytics Inc. for \$~~5,350,6966,190,686~~ for the term of January 1, 2019 through December 31, 2019; and,
- 2) Authorize the Chief Information Officer (CIO) to execute the agreement and to negotiate and execute change orders with Avenu, not to exceed 1540% of the contract amount and within departmental appropriations for IT contract services.

SUMMARY:

The information technology support services contract the County has with Conduent Inc. expires on December 31, 2018. Conduent recently sold its IT outsourcing business to Avenu Insights & Analytics Inc. The County issued a Request for Proposal (RFP) for IT services but Avenu was not able to fully participate in the process due to the status of the sale transaction with Conduent. Additionally, the RFP process yielded only three bidders. In the best interests of the RFP process, and in the interest of providing more choice for the County, the Department suspended the process with the intent of re-issuing the RFP in the new calendar year. Since the current agreement has been assigned to Avenu but expires on December 31, 2018, the Department recommends that the Board approve a 1 year contract extension.

FINANCIAL IMPACT:

The cost of a 12-month extension of the ITSA with Avenu is \$~~5,350,6966,190,686~~. The contract's cost from January 1, 2019 through June 30, 2019 is \$~~2,635,8113,049,599~~ and is included in the Department's budget appropriation for FY2018/19. The cost of extending the ITSA from July 1, 2019 to December 31, 2019 is \$~~2,714,8853,141,987~~ and will be included in the requested budget for FY2019/20. These amounts include base contract services. Current and current, active out of scope work orders that were previously approved this year will be renegotiated separately and fall within the requested 15% contingency for change orders. These amounts are consistent with previous contract amendments and include a COLA as outlined in provisions of the ITSA.

The costs associated with preparing this agenda item are nominal and absorbed by the department's FY2018/19 Adopted Budget.

DISCUSSION:

The County's Information Technology Services Agreement (ITSA) with Conduent Inc. expires on December 31, 2018. The Department issued a Request for Proposal to the IT services marketplace on August 22, 2018. Over 2,000 vendors received notification of the RFP through Public Purchase and over 270 vendors downloaded the RFP documents that were posted to the Public Purchase website. Department staff conducted a pre-proposal bidders conference on September 4, 2018 and nine vendors submitted "Intent to Propose" letters by the September 7th deadline. Proposals were due September 27th.

Although 270 vendors downloaded the RFP documents and nine submitted an intent to propose, only three vendors submitted proposals. In addition, during the RFP process, Conduent was in negotiations to sell its IT services and software business to Avenu Insights & Analytics Inc (which includes services provided under the current agreement). Due to the timing of the sale and the pending RFP, Conduent submitted its proposal on the September 27th deadline and closed the sale of the business to Avenu on September 29th. Subsequent to the sale, the County's agreement with Conduent has been assigned to Avenu. Although the sale was in process for many weeks, Avenu did not participate in formulating the proposal that was submitted by Conduent and it is doubtful that Conduent would now be positioned to fulfill the work outlined in its proposal.

Given the situation with the incumbent service provider, the limited response received from other potential providers, and with concurrence from the County Administrator and County Counsel's Office, the Department suspended the process and withdrew the RFP with the intent to re-issue it as soon as practical.

Given the length of time required by the RFP process, the time required for potential provider transition and the impending retirement of the CIO the Department is recommending that restarting the process wait until the new CIO is in place to manage the process, be involved in the vendor selection, and direct any necessary transition activities.

So that there is not a disruption of service to customers, the Department recommends that the County extend its current ITSA with Avenu for one year.

ALTERNATIVES:

The Board could choose to not approve a 1 year renewal of the ITSA with Avenue, however this is not recommended. The current ITSA expires December 31st and not renewing it would cause disruption to IT service delivery.

The Board could choose to approve an extension to the ITSA for less than one year, however, that is not recommended. Department staff have developed a timeline for restarting the RFP process and estimates that the procurement process would take approximately six months. If the result of the RFP process awards the work to a new provider, an additional six months would be required to affect an orderly transition of services. Additionally, provisions of the ITSA allow the County to off-ramp work or otherwise reduce contractor staffing with only thirty days' notice.

OTHER AGENCY INVOLVEMENT:

The County Administrator's Office and County Counsel's Office have been involved in the decision to suspend the RFP process and renew the ITSA with Avenu for one year. County Counsel's Office has also been involved in the negotiation of ITSA Amendment 10.

CAO RECOMMENDATION:

APPROVE DEPARTMENTAL RECOMMENDATION

Contract Amendment 10
Exhibit A-1

Pricing for the Extension Term of January 1, 2019 through December 31, 2019.

SUMMARY: Extension Term 1/1/19 - 12 /31/19	
Service Recipient:	Solano County
Vendor Name Avenu State and Local	

RECURRING / ONGOING COSTS				
Category	Service / Description	Year 13 Jan 2019 - June 2019	Year 14 July 2019 - Dec 2019	Total
Base Service	Data Center Services	\$236,399	\$243,491	\$479,891
Base Service	Desktop Support Services	\$659,686	\$679,477	\$1,339,162
Base Service	Data Network Services	\$770,085	\$793,187	\$1,563,272
Base Service	GIS Services	\$299,487	\$308,472	\$607,960
Base Service	Help Desk Services	\$136,299	\$140,388	\$276,686
Base Service	Application Services	\$533,854	\$549,870	\$1,083,724
ANNUAL SERVICE FEES		\$2,635,811	\$2,714,885	\$5,350,696

**Contract Amendment 10
Exhibit A-2**

Avenu Provided Staff				01/2019 - 06/2019	07/2019 - 12/2019
Resource Category	Unit of Measure	Baseline Quantity	Monthly Unit Cost	Monthly Total	Monthly Total
Data Center Services					
Management Services	FTE	1	\$ 15,144	\$ 15,144	\$ 15,599
Computer Operator Supervisor	FTE	1	\$ 7,812	\$ 7,812	\$ 8,046
Computer Lead Operator	FTE	1	\$ 7,812	\$ 7,812	\$ 8,046
Computer Lead Operator	FTE	0	\$ 7,812	\$ -	\$ -
Computer Sr Operator	FTE	1	\$ 8,632	\$ 8,632	\$ 8,891
Data Center Services Fees			MONTHLY	\$ 39,400	\$ 40,582
Desktop Support Services					
Management Services	FTE	0.5	\$ 13,327	\$ 6,663	\$ 6,863
Desktop Support Supervisor	FTE	1	\$ 8,784	\$ 8,784	\$ 9,047
System Senior Lead	FTE	1	\$ 8,784	\$ 8,784	\$ 9,047
System Senior Technician	FTE	8	\$ 8,784	\$ 70,270	\$ 72,378
Prod Control Sr. Analyst	FTE	1	\$ 7,724	\$ 7,724	\$ 7,955
Prod Control Analyst	FTE	1	\$ 7,724	\$ 7,724	\$ 7,955
Desktop Support Services Fees			MONTHLY	\$ 109,948	\$ 113,246
Network Services					
Network Supervisor	FTE	1	\$ 16,280	\$ 16,280	\$ 16,768
Security Administration	FTE	1	\$ 15,750	\$ 15,750	\$ 16,223
Network Lead Admin.	FTE	1	\$ 13,024	\$ 13,024	\$ 13,415
Data/Voice Engineers	FTE	2	\$ 15,598	\$ 31,197	\$ 32,133
Network Sr. System Admin.	FTE	4	\$ 13,024	\$ 52,096	\$ 53,659
Network Services Fees			MONTHLY	\$ 128,347	\$ 132,198
HelpDesk Services					
Management Services	FTE	0.5	\$ 13,327	\$ 6,663	\$ 6,863
HelpDesk Lead	FTE	1	\$ 8,026	\$ 8,026	\$ 8,267
HelpDesk Analyst	FTE	1	\$ 8,026	\$ 8,026	\$ 8,267
HelpDesk Services Fees			MONTHLY	\$ 22,716	\$ 23,398
Applications Services					
Management Services	FTE	0	\$ 14,387	\$ -	\$ -
Application Support	FTE	1	\$ 13,630	\$ 13,630	\$ 14,039
DBA Support	FTE	2	\$ 16,441	\$ 32,881	\$ 33,868
Sr. Infrastructure Engineer	FTE	1	\$ 16,356	\$ 16,356	\$ 16,847
Infrastructure Engineer	FTE	1	\$ 13,630	\$ 13,630	\$ 14,039
Systems Development	FTE	1	\$ 12,479	\$ 12,479	\$ 12,853
Applications Services Fees			MONTHLY	\$ 88,976	\$ 91,645
GIS Services					
GIS Programmer/Developer	FTE	1	\$ 13,630	\$ 13,630	\$ 14,039
GIS Analyst - Senior	FTE	1	\$ 13,630	\$ 13,630	\$ 14,039
GIS Analyst	FTE	2	\$ 11,327	\$ 22,655	\$ 23,334
GIS Technician	FTE	0	\$ 11,327	\$ -	\$ -
GIS Services Fees			MONTHLY	\$ 49,915	\$ 51,412
Total Monthly				\$439,302	\$ 452,481
Total for Period				\$2,635,811	\$ 2,714,885

Amended
Contract

Information Technology Services Agreement Amendment 10

County of Solano

Avenu Insights & Analytics Inc.

This tenth amendment ("Amendment No. 10") to the Information Technology Services Agreement dated June 12, 2006 ("Agreement") is made on December 31, 2018 ("Amendment Effective Date"), by and between the County of Solano, California, ("County") and Avenu Insights & Analytics Inc. ("Avenu" or "Provider"). The County and Avenu (each individually a "Party" and collectively "the Parties") agree as follows:

Throughout this Amendment No. 10, wherever language is underlined it is added, and wherever language is ~~crossed-out~~ it is deleted.

1. Section 9.1.4 of the Agreement is deleted and replaced with:

9.1.4 Extended Term

Notwithstanding the expiration of the last Renewal Term pursuant to Sections 9.1.1 and 9.1.2, the Parties agree to extend the term of this Agreement from the Effective Date until December 31, 2019 ("Extension Term").

County shall have the right to extend the Extension Term for up to twelve (12) successive renewal periods of one (1) month (each an "Extension Term") by providing written notice to Provider in accordance with the terms of Section 19.6 Notices at least thirty (30) days before the end of the Extension Term.

2. Schedule 3, Fees, and Appendix 3A of Schedule 3 shall be replaced with the pricing for the Extension Term of January 1, 2019 through December 31, 2019 which is provided in the attached Exhibit A to this Amendment. Should a vacancy occur in one of the identified FTE positions, Contractor agrees that it will only bill 50% for that vacant position for the first full month the position is vacant ("Vacancy Offset"). Should the position remain vacant beyond 30 calendar days, Contractor is not entitled to bill any Vacancy Offset until the position is filled. If a vacant position is filled at any point within a calendar month, Contractor may bill for that pro rata share of the Baseline Quantity that is actually staffed with a qualified FTE. Contractor agrees to provide County with notice of any vacancy within one business day that the vacancy occurs.

In the event the Extension Term continues beyond December 31, 2019, the County and Provider will mutually agree on pricing.

3. Schedule 4, Fee Reductions, shall be deleted and replace with:

Services will be provided subject to (i) availability of resources at any particular time during the Term. The County acknowledges that Avenu is providing a set level of effort based on defined Avenu personnel resources; (ii) the priorities and direction provided by the County; and (iii) the availability of program funding. Any changes in scope, direction or budget that limit or impair Avenu's ability to provide some or all of the Services will result in a reduction in the level of Services.

4. Schedule 2A (Cross Functional Services SOW for Solano County) dated March 14, 2006, and updated on June 07, 2006, is deleted and replaced with the revised Schedule 2A (Modified Cross Functional Services SOW for Solano County) updated December 31, 2018, attached to this Amendment as Exhibit B and made part of the Agreement.

5. Schedule 2D (Data Network Services SOW for Solano County) dated March 14, 2006, and updated on June 06, 2006, is deleted and replaced with the revised Schedule 2D (Data Network Services SOW for Solano County) updated December 31, 2018, attached to this Amendment as Exhibit C and made part of the Agreement.

6. All other terms and conditions set forth in the Agreement, as previously amended, and as amended by this Amendment No. 10, shall remain unchanged and in full effect.

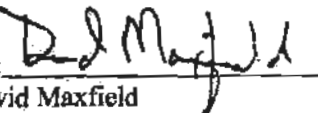
IN WITNESS WHEREOF, County and Provider have caused this Amendment No. 10 to be signed by their duly authorized officers, on the Amendment Effective Date.

County:
County of Solano

By: 

Title: CIO

Provider:
Avenu State & Local

By: 
David Maxfield

Title: CIO & CTO

APPROVED AS TO FORM

By: 
County Counsel

Contract Amendment 10
Exhibit A-1

Pricing for the Extension Term of January 1, 2019 through December 31, 2019.

SUMMARY: Extension Term 1/1/19 - 12/31/19	
Service Recipient:	Solano County
Vendor Name	Avenu State and Local

RECURRING / ONGOING COSTS		Year 13 Jan 2019 - June 2019	Year 14 July 2019 - Dec 2019	Total
Category	Service / Description			
Base Service	Data Center Services	\$236,399	\$243,491	\$479,891
Base Service	Desktop Support Services	\$659,686	\$679,477	\$1,339,162
Base Service	Data Network Services	\$770,085	\$793,187	\$1,563,272
Base Service	GIS Services	\$299,487	\$308,472	\$607,960
Base Service	Help Desk Services	\$136,299	\$140,388	\$276,686
Base Service	Application Services	\$533,854	\$549,870	\$1,083,724
ANNUAL SERVICE FEES		\$2,635,811	\$2,714,885	\$5,350,696

**Contract Amendment 10
Exhibit A-2**

Avenue Provided Staff				01/2019 - 06/2019	07/2019 - 12/2019
Resource Category	Unit of Measure	Baseline Quantity	Monthly Unit Cost	Monthly Total	Monthly Total
Data Center Services					
Management Services	FTE	1	\$ 15,144	\$ 15,144	\$ 15,599
Computer Operator Supervisor	FTE	1	\$ 7,812	\$ 7,812	\$ 8,046
Computer Lead Operator	FTE	1	\$ 7,812	\$ 7,812	\$ 8,046
Computer Lead Operator	FTE	0	\$ 7,812	\$ -	\$ -
Computer Sr Operator	FTE	1	\$ 8,632	\$ 8,632	\$ 8,891
Data Center Services Fees			MONTHLY	\$ 39,400	\$ 40,582
Desktop Support Services					
Management Services	FTE	0.5	\$ 13,327	\$ 6,663	\$ 6,863
Desktop Support Supervisor	FTE	1	\$ 8,784	\$ 8,784	\$ 9,047
System Senior Lead	FTE	1	\$ 8,784	\$ 8,784	\$ 9,047
System Senior Technician	FTE	8	\$ 8,784	\$ 70,270	\$ 72,378
Prod Control Sr. Analyst	FTE	1	\$ 7,724	\$ 7,724	\$ 7,955
Prod Control Analyst	FTE	1	\$ 7,724	\$ 7,724	\$ 7,955
Desktop Support Services Fees			MONTHLY	\$ 109,948	\$ 113,246
Network Services					
Network Supervisor	FTE	1	\$ 16,280	\$ 16,280	\$ 16,768
Security Administration	FTE	1	\$ 15,750	\$ 15,750	\$ 16,223
Network Lead Admin.	FTE	1	\$ 13,024	\$ 13,024	\$ 13,415
Data/Voice Engineers	FTE	2	\$ 15,598	\$ 31,197	\$ 32,133
Network Sr. System Admin.	FTE	4	\$ 13,024	\$ 52,096	\$ 53,659
Network Services Fees			MONTHLY	\$ 128,347	\$ 132,198
HelpDesk Services					
Management Services	FTE	0.5	\$ 13,327	\$ 6,663	\$ 6,863
HelpDesk Lead	FTE	1	\$ 8,026	\$ 8,026	\$ 8,267
HelpDesk Analyst	FTE	1	\$ 8,026	\$ 8,026	\$ 8,267
HelpDesk Services Fees			MONTHLY	\$ 22,716	\$ 23,398
Applications Services					
Management Services	FTE	0	\$ 14,387	\$ -	\$ -
Application Support	FTE	1	\$ 13,630	\$ 13,630	\$ 14,039
DBA Support	FTE	2	\$ 16,441	\$ 32,881	\$ 33,868
Sr. Infrastructure Engineer	FTE	1	\$ 16,356	\$ 16,356	\$ 16,847
Infrastructure Engineer	FTE	1	\$ 13,630	\$ 13,630	\$ 14,039
Systems Development	FTE	1	\$ 12,479	\$ 12,479	\$ 12,853
Applications Services Fees			MONTHLY	\$ 88,976	\$ 91,645
GIS Services					
GIS Programmer/Developer	FTE	1	\$ 13,630	\$ 13,630	\$ 14,039
GIS Analyst - Senior	FTE	1	\$ 13,630	\$ 13,630	\$ 14,039
GIS Analyst	FTE	2	\$ 11,327	\$ 22,655	\$ 23,334
GIS Technician	FTE	0	\$ 11,327	\$ -	\$ -
GIS Services Fees			MONTHLY	\$ 49,915	\$ 51,412
Total Monthly				\$439,302	\$ 452,481
Total for Period				\$2,635,811	\$ 2,714,885

Cost Of Living Adjustment (COLA) – A COLA increase of 3% has been applied to 07/01/19 through 12/31/19 of the schedule

Optional Pricing Modification – At the County's discretion, the Provider offers a value added service to help defray costs associated with this contract. Our clients may access additional revenue generating services to the county such as our Sales and Use Tax services. A portion of the fees incurred under additional services will be credited or applied to the price schedule above. The Sales and Use Tax service utilizes custom software and experienced California Tax Experts to research and recover Solano County tax revenue that was previously not collected or misallocated to other jurisdictions or accounts. This is a completely optional value add that can help self-fund our services.

Contract Amendment 10
Exhibit B

Schedule 2A (Cross Functional Services SOW for Solano County)

Contract Amendment 10
Exhibit C

Schedule 2D (Data Network Services SOW for Solano County)



SCHEDULE 2A
MODIFIED CROSS-FUNCTIONAL SERVICES SOW
for
SOLANO COUNTY

March 14, 2006
Updated June 7, 2006
Updated June 01, 2017
Updated November 29, 2018

Table of Contents

1.0	Cross Functional Services Overview.....	1
2.0	Service Environment	1
2.1	Scope of the Infrastructure to be Supported	1
3.0	Cross Functional Services Requirements.....	1
3.1	Service Descriptions and Roles & Responsibilities	2
3.2	Exclusions	22
4.0	Service Management.....	24
4.1	Objectives.....	24
4.2	Definitions.....	24
4.3	Service Level Requirements (SLRs)	24
4.4	Reports.....	27
5.0	List of Referenced MSA Schedules.....	27

List of Tables

Table 1.	General Services Roles and Responsibilities	2
Table 2.	Planning and Analysis Roles and Responsibilities	3
Table 3.	Requirements Definition Roles and Responsibilities	4
Table 4.	Design Specifications Roles and Responsibilities	5
Table 5.	Engineering/Development Roles and Responsibilities.....	6
Table 6.	Integration and Testing Roles and Responsibilities	6
Table 7.	Implementation and Migration Roles and Responsibilities	7
Table 8.	Environmental and Facilities Support Roles and Responsibilities.....	8
Table 9.	Training and Knowledge Transfer Roles and Responsibilities	9
Table 10.	Documentation Roles and Responsibilities	10
Table 11.	Operations and Administration Roles and Responsibilities	11
Table 12.	Maintenance Roles and Responsibilities	12
Table 13.	Technology Refreshment and Replenishment Roles and Responsibilities	13
Table 14.	Service Level Monitoring and Reporting Responsibilities	14
Table 15.	IT Service Continuity and Disaster Recovery Services Roles and Responsibilities.....	15
Table 16.	Financial/Chargeback Management and Invoicing Roles and Responsibilities.....	16
Table 17.	Incident & Problem Management Roles and Responsibilities	16
Table 18.	Root Cause Analysis Roles and Responsibilities	18
Table 19.	Configuration Management Roles and Responsibilities.....	18
Table 20.	Change and Release Management Roles and Responsibilities.....	20
Table 21.	Account Management Roles and Responsibilities.....	21
Table 22.	Monitoring, Reporting and Review Roles and Responsibilities	22

Table 23.	Incident Resolution SLRs	24
Table 24.	Priority Levels	25
Table 25.	Backup Schedule	25
Table 26.	Restoration SLR	26
Table 27.	Cross Functional Services Reports	27

This is Schedule 2.A (Cross Functional Services SOW) to the Agreement between Solano County ("County") and Provider. Unless otherwise expressly defined herein, the capitalized terms used herein shall have the meaning assigned to them in Attachment A2 (SOW Definitions) or in the Agreement.

1.0 Cross Functional Services Overview

This Schedule 2A (Cross Functional Services SOW) is the Statement of Work (or "SOW") that sets forth the roles and responsibilities of the Parties for the set of common services that apply to the provision, delivery, and management of all Services ("Cross Functional Services") in support of the County Information Technology (IT) infrastructure. Provider will provide Cross Functional Services across all in-scope Service Towers. As depicted in Figure 1 below, Services, activities and roles and responsibilities described in this SOW are within the scope of each SOW for the Service Towers (Schedules 2A through 2F) and shall be included within the Fees for each Service Tower specified in Schedule 3 (Fees) to the Agreement. Provider shall provide all hardware, software, and infrastructure support in connection with all Bundled Service Component(s). As of the effective date of the Agreement, the County is responsible for providing all other hardware, software, and infrastructure necessary for provider to deliver all Services under this Agreement.

Figure 1 depicts the relationship between the Cross Functional Services SOW, and all SOWs within the scope of the Agreement.

Figure 1: SOW Service Towers with Cross Functional View



2.0 Service Environment

2.1 Scope of the Infrastructure to be Supported

The Service Environment section in Service Tower SOW describes the environment to be supported and/or with which Provider shall comply. The Service Environment includes Service Tower components such as hardware and software, facilities and locations, personnel, policies and procedures, licenses and agreements. As such, this SOW shall apply to the Service Environment as specified in each Service Tower SOW, with the exception of work-in-progress and future initiatives which will be described in this SOW. The Service Environment for each Service Tower will be documented in the applicable SOW Appendices and are to be maintained by Provider, reviewed with the County, updated by Provider and made available to the County on a quarterly basis.

3.0 Cross Functional Services Requirements

The Provider is responsible for providing Cross Functional Services defined in this SOW for Service Towers defined in the following documents:

- Modified Schedule 2B – Data Center Services SOW
- Modified Schedule 2C – Desktop Support Services SOW
- Schedule 2D – Server Administration Services SOW
- Modified Schedule 2E – Help Desk Services SOW
- Modified Schedule 2F – Application Services SOW

3.1 Service Descriptions and Roles & Responsibilities

IT Lifecycle & Operations	Service Delivery	Service Support
<ul style="list-style-type: none"> Planning & Analysis Requirements Definition Integration & Testing Implementation & Migration Environment & Facilities Support Training & Knowledge Transfer Documentation Operations & Administration Maintenance Technology Refreshment & Replenishment 	<ul style="list-style-type: none"> Capacity Management Performance Management Service Level Monitoring & Reporting IT Service Continuity & Disaster Recovery Financial/Chargeback Management & Invoicing 	<ul style="list-style-type: none"> Incident & Problem Management Root Cause Analysis Configuration Management Change & Release Management Account Management

3.1.1 General Responsibilities

The following table identifies General roles and responsibilities associated with this SOW. An "X" is placed in the column under the Party that will be responsible for performing the task. Provider responsibilities are indicated in the column labeled "Provider."

Table 1. General Services Roles and Responsibilities

General Roles and Responsibilities	Provider	County
1. Perform business liaison function for County operational units		X
2. Provide Services that support County business needs, technical requirements and End-User requirements	X	
3. Comply with County policies and standards and regulations applicable to the County for information, information systems, personnel, physical security	X	
4. Develop and maintain a comprehensive Procedures Manual that contains the operational procedures that will be used in the delivery of Services	X	
5. Conform to changes in laws, regulations and policies. Major changes shall be proposed on a project-by-project effort basis to alter the environment to conform to the new requirements	X	

General Roles and Responsibilities	Provider	County
6. Report performance against Service Level Requirements (SLRs) as applicable	X	
7. Coordinate all changes to the IT infrastructure that may affect the SLRs of any other Service Tower apart from Data Networking and Security Infrastructure	X	
8. Provide timely creation, updating, maintenance and provision of all appropriate project plans, project time and cost estimates, technical Specifications, management documentation and management reporting in a form/format that is acceptable to the County for all Service Tower projects and major service activities		X
9. Provide time and cost estimates, technical specifications, management documentation and management reporting in a form/format that is acceptable to the County for all Service Tower projects and major service activities	X	
10. Adhere to ITIL best practices	X	
11. Provide support for financial audits	X	

3.1.2 IT Lifecycle & Operations

3.1.2.1 Planning and Analysis

Planning and Analysis Services are activities associated with researching new technical trends, products and services, such as hardware components, and System Software, that offer opportunities to improve the efficiency and effectiveness of the Service Towers. Planning and Analysis Services can also help mitigate risks by reducing defects and improving the Quality of IT Services. The following table identifies the Planning and Analysis roles and responsibilities that Provider and the County will perform.

Table 2. Planning and Analysis Roles and Responsibilities

Planning and Analysis Roles and Responsibilities	Provider	County
1. Define Services, standards and timeframes for Planning and Analysis activities		X
2. Participate in defining Services and standards for Planning and Analysis activities	X	
3. Review and approve Services and standards for Planning and Analysis activities		X
4. Define County requirements at the enterprise level for all Service Towers (e.g., business, technology strategy, functional, availability, capacity, performance, backup and IT continuity service)		X
5. Perform infrastructure, configuration, technical and Service Planning and Analysis based on County requirements (e.g., Availability, capacity, performance, backup and IT Continuity and Disaster Recovery Services) apart from Data Network and Security Infrastructure	X	
6. Provide infrastructure installation and upgrade recommendations	X	

Planning and Analysis Roles and Responsibilities	Provider	County
7. Approve infrastructure Planning and Analysis and recommendations for new applications, infrastructure and Services		X
8. Provide management reports required for Planning and Analysis activities (e.g., utilization and capacity trend reports)	X	
9. Define County Data Backup and Retention requirements and policies for all Service Towers		X
10. Recommend Data Backup and Retention process for meeting the County requirements	X	
11. Continuously monitor technical trends through independent research; document and report on products and services with potential use for the County as it aligns with the County's business and technology strategy	X	
12. Perform feasibility studies for the implementation of new technologies that best meet County business needs and meet cost, performance and Quality objectives	X	
13. Define enterprise-level project management policies, procedures and requirements (e.g., project feasibility analysis, cost benefit analysis, scheduling, costing, resource planning, communication planning, procurement, risk management and Quality management)		X
14. Perform project management oversight and liaison function to the business and customers		X
15. Conduct technical and business planning sessions to establish standards, architecture and project initiatives		X
16. Participate in technical and business planning sessions to establish standards, architecture and project initiatives	X	
17. Conduct regular planning for technology refresh and upgrades	X	
18. Participate in regular planning for technology refresh and upgrades		X
19. Conduct technical reviews and provide recommendations for improvements to the infrastructure that increase efficiency and effectiveness and reduce costs	X	

3.1.2.2 Requirements Definition

Requirements Definition services are the activities associated with the assessment and definition of functional, performance, IT Continuity and Disaster Recovery, and requirements that also comply with regulatory and County policies. These requirements drive the technical design for the environment. The following table identifies the Requirements Definition roles and responsibilities that Provider and the County will perform.

Table 3. Requirements Definition Roles and Responsibilities

Requirements Definition Roles and Responsibilities	Provider	County
1. Define requirements standards		X
2. Participate in defining requirements and standards	X	

Requirements Definition Roles and Responsibilities	Provider	County
3. Conduct interviews, group workshops, and surveys to determine user functional, performance, availability, maintainability and IT continuity requirements		X
4. Participate in appropriate requirements gathering activities (e.g., focus groups, interviews)	X	
5. Provide written information pertaining to the requirements definition to enable development of appropriate requirements documentation (e.g., business requirements documentation)		X
6. Document all requirements in agreed to formats (e.g., system Specifications, data models,)	X	
7. Approve all requirements documents		X
8. Define Acceptance test criteria		X
9. Participate in defining and document Acceptance test criteria	X	
10. Review and approve all Acceptance test criteria		X

3.1.2.3 Design Specifications

Design Specification services are the activities and deliverables associated with translating user and information system requirements into detailed technical Specifications. The following table identifies the Design Specifications roles and responsibilities that Provider and the County will perform.

Table 4. Design Specifications Roles and Responsibilities

Design Specification Roles and Responsibilities	Provider	County
1. Define Design Specifications standards and requirements		X
2. Develop and document technical design plans and environment configuration based on County Design Specifications standards and requirements, including IT architecture, functional, performance, availability, maintainability, and IT Continuity and Disaster Recovery requirements	X	
3. Determine required upgrade, replacement and/or conversion requirements (e.g., hardware, Software)	X	
4. Review and approve design plans through coordination with the appropriate County technology standards group and design architects		X
5. Conduct site surveys for design efforts as required	X	
6. Provide written information in sufficient detail pertaining to the Design Specifications to enable Provider to create the appropriate design documents		X
7. Document and deliver Design Specifications	X	
8. Review and approve Design Specifications		X

3.1.2.4 Engineering/Development

Engineering/Development services are the activities associated with the engineering and development of the IT infrastructure, tools and utilities that enhance the IT Infrastructure. The following table identifies the Engineering/Development roles and responsibilities that Provider and the County will perform.

Table 5. Engineering/Development Roles and Responsibilities

Engineering/Development Roles and Responsibilities	Provider	County
1. Recommend Engineering/Development requirements and policies	X	
2. Review and approve Engineering/Development requirements and policies		X
3. Develop and document in the Procedures Manual Engineering/Development procedures that meet requirements and adhere to defined policies	X	
4. Develop and deliver Engineering/Development plans where there is an impact on County entities/facilities and/or other third-party agreements	X	
5. Perform engineering functions required to implement design plans for additional or new products and services	X	
6. Perform engineering functions required to implement and manage IT Infrastructure services on County owned/leased facilities	X	
7. Manage engineering/development efforts using formal project management tools and methodologies		X
8. Review and approve Engineering/Development plans and procedures		X

3.1.2.5 Integration and Testing

Integration and Testing services are the activities associated with ensuring that all individual IT components configured with or added to the IT infrastructure work together cohesively to achieve the intended results. The following table identifies the Integration and Testing roles and responsibilities that Provider and the County will perform.

Table 6. Integration and Testing Roles and Responsibilities

Integration and Testing Roles and Responsibilities	Provider	County
1. Define Integration and Testing requirements and policies		X
2. Develop and document in the Procedures Manual the Integration and Testing procedures that meet requirements and adhere to defined policies	X	
3. Review and approve Integration and Testing procedures		X
4. Manage integration test environment	X	
5. Maintain systems Software release matrices across development, QA, and production environments	X	
6. Validate and approve the Software release and version level		X

Integration and Testing Roles and Responsibilities	Provider	County
7. Conduct integration testing for all new and upgraded equipment, Software or services to include unit, system, integration and regression testing, as applicable	X	
8. Evaluate all new and upgraded IT Infrastructure components for compliance with County, regulations and procedures	X	
9. Assess and communicate the overall impact and potential risk to IT Infrastructure components prior to implementing changes	X	
10. Coordinate integration and testing activities with applications support	X	
11. Define User Acceptance Test (UAT) requirements and plans		X
12. Conduct User Acceptance Test (UAT) and document results		X
13. Stage new and upgraded equipment, Software or services to smoothly transition into existing environment	X	
14. Perform modifications and performance-enhancement adjustments to County system Software and utilities as a result of changes to architectural standards	X	
15. Test new releases of supported hardware and systems Software to ensure conformance with County SLRs	X	
16. Perform configuration management and change management activities related to Integration and Testing	X	

3.1.2.6 Implementation and Migration

Implementation and Migration services are the activities associated with the installation of new and upgraded IT components (e.g., hardware, Software) into the production environment. The following table identifies the Implementation and Migration roles and responsibilities that Provider and the County will perform.

Table 7. Implementation and Migration Roles and Responsibilities

Implementation and Migration Roles and Responsibilities	Provider	County
1. Define Implementation and Migration requirements and policies		X
2. Develop and document in the Procedures Manual the Implementation and Migration procedures that meet requirements and adhere to defined policies	X	
3. Review and approve Implementation and Migration procedures		X
4. Notify Provider of equipment migration and redeployment plans		X
5. Coordinate and review all Implementation and Migration plans and schedules with the County in advance in accordance with Change Management Policies	X	
6. Approve Implementation and Migration plans and schedules		X
7. Install new IT Infrastructure components and perform upgrades as a result of new and enhanced tools and technologies (e.g., hardware, systems Software, utilities, peripherals, configurations)	X	

Implementation and Migration Roles and Responsibilities	Provider	County
8. Coordinate Implementation and Migration support activities with County IT staff and the Help Desk	X	
9. Perform data migration per County requirements, (e.g., databases, repositories)	X	
10. Perform appropriate tests on all installs, moves, adds and changes	X	
11. Conduct User Acceptance Tests (UAT) and document results	X	
12. Support User Acceptance Tests (UAT)		X
13. Provide County IT technical staff and End-Users with training related to the implementation of new products and services	X	

3.1.2.7 Environment and Facilities Support

Environment and Facilities Support Services are the activities associated with maintaining environmental requirements at the County facilities. The following table identifies Environment and Facilities Support roles and responsibilities that Provider and the County will perform.

Table 8. Environmental and Facilities Support Roles and Responsibilities

Environmental and Facilities Support Roles and Responsibilities	Provider	County
1. Recommend Environment and Facilities Support requirements and policies	X	
2. Review and approve Environment and Facilities Support requirements and policies		X
3. Develop and document in the Procedures Manual the Environment and Facilities Support procedures that meet requirements and adhere to defined policies	X	
4. Review and approve Environment and Facilities Support procedures		X
5. Monitor environmental systems (e.g., UPS) required to support IT Infrastructure components housed in County facilities (e.g., computer rooms)	X	
6. Develop and recommend improvement plans for County facilities as needed to maintain an effective and secure computing environment	X	
7. Approve the improvement plans		X
8. Coordinate the implementation of all approved upgrades and installations	X	
9. Coordinate County site activities of all personnel (i.e., Provider employees and others) working in equipment locations (e.g., equipment rooms)	X	
10. Ensure that facilities support activities conform to the requirements of the defined Change Management processes	X	

3.1.2.8 Training and Knowledge Transfer

Training and Knowledge Transfer Services consist of the following three types of training Provider will perform:

- a. Training for the improvement of skills through education and instruction for Provider's staff. Provider will participate in any pertinent initial and on-going training delivered by the County as required that would provide a learning opportunity about the County's business and technical environment
- b. Training for County technical staff for the express purpose of exploitation of the functions and features of the County computing environment. Delivery methods may include classroom style, computer-based, individual, or other appropriate means of instruction.

The following table identifies the Training and Knowledge Transfer roles and responsibilities that Provider and the County will perform.

Table 9. Training and Knowledge Transfer Roles and Responsibilities

Training and Knowledge Transfer Roles and Responsibilities	Provider	County
1. Define Training and Knowledge Transfer requirements and policies		X
2. Develop and document in the Procedures Manual, Training and Knowledge Transfer procedures that meet requirements and adhere to defined policies	X	
3. Review and approve Training and Knowledge Transfer procedures		X
4. Develop, implement and maintain a County accessible knowledge database/portal	X	
5. Develop and implement knowledge transfer procedures to ensure that more than one individual understands key components of the business and technical environment	X	
6. Prepare materials and deliver training to Provider's personnel on County business and technical environments		X
7. Participate in County delivered instruction on the business and technical environment	X	
8. Develop, document and deliver training to County support staff for ongoing provision of County services, including refresher courses as needed and instruction on new functionality	X	
9. Provide County and Provider support staff with training needed to remain current with systems, Software, features and functions for which IT Infrastructure support is provided in order to improve service performance	X	
10. Provide assistance to HR for New Employee orientation as it pertains to IT in the County.	X	
11. Develop training and knowledge transfer plan in the project plan		X
12. Approve training and knowledge transfer plan in the project plan		X
13. Provide technical training assistance and knowledge transfer to existing County support personnel, during deployment as requested	X	

Training and Knowledge Transfer Roles and Responsibilities	Provider	County
14. Provide End-User training content for County Applications		X
15. Review and validate training content		X
16. Provide continuing End-User training for improving "how-to-use" skills related to systems and applications	X	
17. Create and maintain County Training instances or clients as required by the County	X	
18. Provide Help desk agent training, including developing dialogue scripts	X	

3.1.2.9 Documentation

Documentation Services are the activities associated with developing, revising, maintaining, reproducing, and distributing IT Infrastructure services information in hard copy and electronic form. The following table identifies the Documentation roles and responsibilities that Provider and the County will perform.

Table 10. Documentation Roles and Responsibilities

Documentation Roles and Responsibilities	Provider	County
1. Recommend Documentation requirements and formats	X	
2. Approve Documentation requirements, formats and policies		X
3. Develop and document in the Procedures Manual the Documentation procedures that meet requirements and adhere to defined policies	X	
4. Provide County-specific operating requirements		X
5. Document standard operating procedures (e.g., boot, failover, spool management, batch processing, backup)	X	
6. Document policies, procedures, production & maintenance schedules and job schedules	X	
7. Provide output in agreed format for support of activities throughout the life cycle of services as specified in each Service Tower	X	
8. Recommend specifications and documentation format and content per requirements	X	
9. Approve documentation format and content		X
10. Provide system specifications and documentation	X	
11. Develop operational processing flow	X	
12. Provide system installation, support, configuration and tuning manuals	X	
13. Provide application hardware and system software requirements documentation	X	
14. Provide logical and physical data model	X	
15. Provide End-User documentation		X
16. Provide standard operating procedures	X	
17. Prepare updates and release notes	X	

Documentation Roles and Responsibilities	Provider	County
18. Deliver updates and release notes to End Users		X
19. Document version control for all documentation for which Provider is responsible	X	
20. Provide documented application disaster recovery process	X	
21. Approve documented application disaster recovery process		X
22. Approve documentation delivered		X

3.1.2.10 Operations and Administration

Operations and Administration Services are the activities associated with providing a stable IT infrastructure and effectively and efficiently performing those activities to ensure IT Services meet SLR targets and requirements. The following table identifies the Operations and Administration roles and responsibilities that Provider and the County will perform.

Table 11. Operations and Administration Roles and Responsibilities

Operations and Administration Roles and Responsibilities	Provider	County
1. Provide Operations and Administration requirements and policies, including schedules for the operation of County IT Infrastructure		X
2. Develop and document in the Procedures Manual the Operations and Administration procedures that meet requirements and adhere to defined policies	X	
3. Develop operational documentation (e.g., Run Books, Contact Lists, Operations scripts) that meets County requirements	X	
4. Review and approve Operations and Administration procedures and operational documentation		X
5. Identify and recommend Enterprise System Management tools to monitor the IT infrastructure	X	
6. Approve and provide enterprise System Management tools to monitor the IT infrastructure		X
7. Coordinate with the County to deploy enterprise IT Infrastructure management tools to monitor the operation of the infrastructure	X	
8. Install and configure enterprise IT Infrastructure management tools for a shared use environment. The Problems, issues and events are proactively identified, reported and resolved according to prescribed SLRs	X	
9. Perform event management monitoring of IT Infrastructure Services to detect abnormal conditions or alarms, log abnormal conditions, analyze the condition and take corrective action	X	
10. Manage hardware, Software, peripherals, services and spare parts to meet SLRs, minimize down time and minimize County resource requirements	X	
11. Interface with Help Desk and the County for Incident & Problem Management activities	X	

Operations and Administration Roles and Responsibilities	Provider	County
12. Provide Level 2 and Level 3 support as required	X	
13. Manage and coordinate subcontractors and third parties in order to meet Service and SLR requirements	X	
14. Develop and provide operational reports (Daily, Weekly, Monthly) that provide status of operational activities, production issues, and key operational metrics	X	
15. Review operational reports		X
16. Provide recovery and backup requirements and updates as they change		X
17. Manage backup media inventory (Tape, Disk, Optical and other media type) including the ordering and distribution of media	X	
18. Perform IT Infrastructure backups and associated rotation of media	X	
19. Provide exception report explaining why any backup failed and steps which will be taken to resolve current failure and prevent future failures	X	
20. Archive data media at a secure off-site location	X	
21. Ensure ongoing capability to recover archived data from media as specified (backwards compatibility of newer backup equipment)	X	
22. Test backup media to ensure incremental and full recovery of data is possible and ensure IT Infrastructure integrity as required or requested by the County	X	
23. Recover files, file system or other data required from backup media as required or requested by the County	X	
24. Conduct disaster recovery testing per policies and procedures	X	
25. Audit Operations and Administration policies for compliance with County security policies		X
26. Provide the County with a copy of or access to any vendor-supplied documentation (including updates thereto)	X	

3.1.2.11 Maintenance

Maintenance Services are the activities associated with the maintenance and repair of hardware, Software to include "break-and-fix" Services. Installed platform and product version levels are not to be more than one version behind the current commercial release, unless specified by the County. The following table identifies the Maintenance roles and responsibilities that Provider and the County will perform.

Table 12. Maintenance Roles and Responsibilities

Maintenance Roles and Responsibilities	Provider	County
1. Define Maintenance requirements and policies		X
2. Develop and document in the Procedures Manual the Maintenance procedures that meet requirements and adhere to defined policies	X	
3. Develop Maintenance schedules	X	

Maintenance Roles and Responsibilities	Provider	County
4. Review and approve Maintenance procedures and schedules		X
5. Update maintenance requirements and point-of-service locations		X
6. Ensure appropriate Maintenance coverage for all IT Infrastructure components, including coordinating with 3rd party vendors	X	
7. Provide maintenance and Break/Fix support in the County's defined locations, including dispatching repair technicians to the point-of-service location if necessary	X	
8. Perform diagnostics and maintenance on IT Infrastructure components including hardware, Software, peripherals, and special purpose devices as appropriate	X	
9. Install manufacturer field change orders, service packs, product patches, firmware, and Software maintenance releases, etc.	X	
10. Perform electronic Software distribution and version control	X	
11. Perform preventive maintenance according to the manufacturers' recommendations	X	
12. Conduct maintenance and parts management and monitoring during warranty and off-warranty periods	X	

3.1.2.12 Technology Refreshment and Replenishment

Technology Refreshment and Replenishment (TR&R) are the activities associated with modernizing the IT infrastructure on a continual basis to ensure that the IT Infrastructure components stay current with evolving industry standard technology platforms. The following table identifies the Technology Refreshment and Replenishment roles and responsibilities that Provider and the County will perform.

Table 13. Technology Refreshment and Replenishment Roles and Responsibilities

TR&R Roles and Responsibilities	Provider	County
1. Define TR&R life-cycle management policies, procedures and plans appropriate for support of County business requirements		X
2. Develop and document in the Procedures Manual the TR&R procedures and plans that meet requirements and adhere to defined policies	X	
3. Review and approve TR&R procedures and plans		X
4. Manage, maintain, and update approved TR&R policies, procedures, and plans	X	
5. Perform the necessary tasks required to fulfill the TR&R plans in accordance with the Change Management process	X	
6. Provide management reports on the progress of the TR&R plans	X	
7. Periodically review the approved TR&R implementation plans to ensure they properly support County business requirements		X

3.1.3 Service Delivery

The following table identifies the Capacity Management roles and responsibilities that Provider and the County will perform.

3.1.3.1 Service Level Monitoring and Reporting

Service Level Monitoring and Reporting Services are the activities associated with the monitoring and reporting of Service delivery with respect to SLRs. In addition, Provider shall report system management information (e.g., performance metrics, and system utilization) to the designated County representatives in a format agreed to by the County. The following table identifies the Service Level Monitoring and Reporting roles and responsibilities that Provider and the County will perform.

Table 14. Service Level Monitoring and Reporting Responsibilities

Service Level Monitoring Roles and Responsibilities	Provider	County
1. Define Service Level requirements		X
2. Perform Monitoring according to the guidelines established in the SLRs.	X	
3. Coordinate SLR monitoring and reporting with designated County representatives and third-party vendors	X	
4. Measure, analyze, and provide management reports on performance relative to SLRs	X	
5. Develop and deliver SLR improvement plans where appropriate	X	
6. Review and approve SLR improvement plans		X
7. Implement SLR improvement plans and report on results	X	
8. Review and approve SLR metrics and performance reports		X
9. Provide County electronic access to performance and SLR reporting and monitoring system	X	
10. Perform audits of SLR results		X
11. Assist in audits of SLR results	X	

3.1.3.2 IT Service Continuity and Disaster Recovery (DR) Services

IT Service Continuity and Disaster Recovery (DR) Services are the activities associated with providing IT Service Continuity and DR Services for prioritized County applications and their associated infrastructure (e.g., CPU, servers, data and output devices, End-User devices) and for County applications and associated infrastructure will receive DR Services according to County Business Impact Analysis (BIA) Document. Provider must demonstrate that it will consistently meet County IT Service Continuity and Disaster Recovery Services requirements. The following table identifies Service Continuity and Disaster Recovery Services roles and responsibilities that Provider and the County will perform.

Table 15. IT Service Continuity and Disaster Recovery Services Roles and Responsibilities

IT Service Continuity and Disaster Recovery Services Roles and Responsibilities	Provider	County
1. Define IT Service Continuity and Disaster Recovery Services strategy, requirements and policies		X
2. Recommend best practices for IT Service Continuity and Disaster Recovery Services strategies, policies and procedures	X	
3. Document IT Service Continuity and Disaster Recovery Services procedures that adhere to County requirements and policies	X	
4. Review and approve IT Service Continuity and Disaster Recovery Services procedures		X
5. As needed, assist the County in other IT continuity and emergency management activities	X	
6. Develop and maintain a detailed DR plan to achieve IT Service Continuity and Disaster Recovery requirements, encompassing data back-ups, storage management and contingency operations that provide for the recovery of the County's systems within established recovery requirement timeframes	X	
7. Define data (File System, Database, Flat Files etc.) replication, backup and retention requirements		X
8. Establish processes to ensure DR plans are kept up to date and reflect changes in the County environment	X	
9. Review & approve DR plans		X
10. Establish DR test requirements		X
11. Perform scheduled DR tests per County policies	X	
12. Coordinate involvement of users for DR testing		X
13. Participate in DR tests		X
14. Track and report DR test results to the County	X	
15. Review & approve DR testing results		X
16. Develop action plan to address DR testing results	X	
17. Review and approve action plan		X
18. Implement action plan and provide ongoing status until completion	X	
19. Initiate the DR plan in the event of a County DR situation per the DR policies and procedures		X
20. Initiate the DR plan in the event of a Provider site DR situation and notify the County per DR policies and procedures	X	
21. Coordinate with the County during a Provider site DR situation per DR policies and procedures	X	

3.1.3.3 Financial/Chargeback Management and Invoicing

Financial/Chargeback Management and Invoicing Services are the activities associated with providing both data that enables the County to charge back its internal business units for usage

of IT Resources and accurate invoices that meet County requirements. The following table identifies the Financial/Chargeback Management and Invoicing roles and responsibilities that Provider and the County will perform.

Table 16. Financial/Chargeback Management and Invoicing Roles and Responsibilities

Financial/Chargeback Management and Invoicing Roles and Responsibilities	Provider	County
1. Define Financial/Chargeback Management and Invoicing requirements and policies		X
2. Develop and document in the Procedures Manual the Financial/Chargeback Management and Invoicing procedures that meet requirements and adhere to defined policies		X
3. Provide chargeback data and reports to enable the County to perform chargeback	X	
4. Review chargeback reports		X
5. Identify invoicing requirements		X
6. Document and maintain invoicing requirements		X
7. Issue invoices and/or journal transactions		X

3.1.4 Service Support

3.1.4.1 Incident & Problem Management

Incident and Problem Management Services are the activities associated with restoring normal Service operation as quickly as possible and to minimize any adverse impact on County business operations, thus ensuring that the best possible levels of Service Quality and Availability are maintained.

Problem Management also includes minimizing the adverse impact of Incidents and Problems on the business that are caused by errors in the IT infrastructure and preventing the recurrence of Incidents related to those errors. In order to achieve this goal, Problem Management seeks to get to the Root Cause of Incidents and then initiate actions to improve or correct the situation. The following table identifies the Incident and Problem Management roles and responsibilities that Provider and the County will perform.

Table 17. Incident & Problem Management Roles and Responsibilities

Incident and Problem Management Roles and Responsibilities	Provider	County
1. Define Incident and Problem Management requirements and policies		X
2. Develop and document in the Procedures Manual the Incident and Problem Management procedures that meet requirements and adhere to defined policies	X	
3. Review and approve Incident and Problem Management requirements and policies		X
4. Establish operations and service management Quality assurance and control programs	X	

Incident and Problem Management Roles and Responsibilities	Provider	County
5. Review and approve operations and service management Quality assurance and control programs		X
6. Execute Quality assurance and Quality control programs	X	
7. Coordinate user support activities with the Help Desk	X	
8. Establish Incident/Problem classification by priority		X
9. Establish Incident/Problem workflow, escalation, communication and reporting processes that help to achieve the SLR requirements	X	
10. Review and approve Incident/Problem workflow, escalation, communication and reporting processes		X
11. Provide, configure, and operate Incident and Problem management system that tracks Incidents across all IT towers	X	
12. Provide County access and input capabilities to Incident and Problem tracking system to allow for Incident/Problem monitoring and ad hoc reporting	X	
13. Manage entire Incident/Problem lifecycle including detection, diagnosis, status reporting, repair and recovery	X	
14. Ensure Incident Resolution activities conform to defined Change Management procedures	X	
15. Manage efficient workflow of Incident resolution, including the involvement of third-party Providers (e.g., vendors, public carriers, ISP)	X	
16. Coordinate and take ownership of Problem resolution with the County and third parties (e.g., public carriers, ISP)	X	
17. Periodically review the state of open Problems and the progress being made in addressing Problems		X
18. Participate in Problem review sessions and provide listing and status of Problems categorized by Problem impact	X	
19. Authorize close of County-initiated Priority 1 and 2 Incidents		X
20. Identify possible enhancement opportunities for improved operational performance and potential cost savings	X	
21. Review and approve projects to implement enhancement opportunities		X

3.1.4.2 Root Cause Analysis

Provider will develop, implement, and maintain a Root Cause Analysis (RCA) process and perform the activities required to diagnose, analyze, recommend and take corrective measures to prevent recurring Problems and/or trends. The following table identifies Root Cause Analysis roles and responsibilities that Provider and the County will perform.

Table 18. Root Cause Analysis Roles and Responsibilities

Root Cause Analysis Roles and Responsibilities	Provider	County
1. Define RCA requirements and policies		X
2. Develop and document in the Procedures Manual the RCA procedures that meet requirements and adhere to defined policies	X	
3. Review and approve RCA procedures		X
4. Conduct proactive trend analysis to identify recurring Problems	X	
5. Track and report recurring Problems or failures and provide business impact analysis of Problems to the County	X	
6. Recommend solutions to address recurring Problems or failures	X	
7. Review and approve solutions to address recurring Problems or failures		X
8. Flag all Priority Levels 1 and 2 Incidents that require Root Cause Analysis	X	
9. Identify root cause of Priority Levels 1 and 2 Incidents and recommend appropriate resolution action	X	
10. Review and approve solutions to address Priority Levels 1 and 2 Incidents		X
11. Provide status report detailing the root cause of and procedure for correcting recurring Problems and Priority Levels 1 and 2 Incidents until closure as determined by the County	X	

3.1.4.3 Configuration Management

Configuration Management Services are the activities associated with providing an integrated set of IT Infrastructure components that work together with reliability, consistency, predictability and manageability. IT Infrastructure configurations need to be modeled and tracked in order to account for all IT assets, provide accurate information on configurations and provide a sound basis for Incident, Problem, Change and Release Management. The following table identifies the Configuration Management roles and responsibilities that Provider and the County will perform.

Table 19. Configuration Management Roles and Responsibilities

Configuration Management Roles and Responsibilities	Provider	County
1. Define Configuration Management requirements and policies		X
2. Develop and document in the Procedures Manual the Configuration Management procedures that meet requirements and adhere to defined policies	X	
3. Review and approve Configuration Management procedures and processes		X
4. Recommend Configuration Management tool set	X	
5. Approve and Provide Configuration Management database and tools		X
6. Establish and maintain Configuration Management database and tools	X	

Configuration Management Roles and Responsibilities	Provider	County
7. Enter/upload configuration data into configuration database	X	
8. Establish process interfaces to Problem & Incident management, change management, technical support, maintenance and asset management processes	X	
9. Establish appropriate authorization controls for modifying configurations	X	
10. Determine impact of configuration changes on Software licensing	X	
11. Establish guidelines for physical and logical separation between development, test and production and the process for deploying and back out of configuration changes	X	
12. Establish configuration Baselines as reference points for rebuilds and provide ability to revert to stable configuration states	X	
13. Establish process for verifying the accuracy of configuration data, adherence to configuration management process and identifying process deficiencies	X	
14. Provide configuration management reports as required and defined by the County	X	
15. Audit configuration management process and accuracy of configuration data		X

3.1.4.4 Change and Release Management

Change Management Services are activities associated with ensuring that standardized methods and procedures are used for efficient and prompt handling of all changes, in order to minimize the impact of change upon Service Quality. Change Management covers all aspects of managing the introduction and implementation of changes affecting the IT Infrastructure, including changes to management processes, tools, and methodologies designed and utilized to support the IT Infrastructure. The Change Management process includes the following sub-processes:

- Request process
- Recording/Tracking process
- Prioritization process
- Responsibility Assignment process
- Impact/Risk Assessment process
- Review / Approval process
- Implementation process
- Verification (test) process
- Release process
- Closure process

Release Management Services are activities associated with bundling multiple changes into one, organized release set to improve manageability of changes. Release Management ensures

that all aspects of a release, both technical and non-technical are considered together and planned methodically to result in successful, non-disruptive implementation. These activities ensure that only correct, authorized and tested versions are installed and that changes are traceable and secure.

The following table identifies Change and Release Management roles and responsibilities that Provider and the County will perform.

Table 20. Change and Release Management Roles and Responsibilities

Change and Release Management Roles and Responsibilities	Provider	County
1. Define Change and Release Management requirements and policies		X
2. Develop and document in the Procedures Manual the Change and Release Management procedures that meet requirements and adhere to defined policies	X	
3. Review and approve Change and Release Management procedures		X
4. Secure and maintain master copies of new Software versions in a Software library and update configuration databases	X	
5. Establish change classifications (impact, priority, risk) and change authorization process		X
6. Administer the version control process as it relates to Release management	X	
7. Review release notes and establish plans (e.g., back out plan, go/no go decision) as appropriate to meet the needs of the County	X	
8. Document and classify proposed changes to the environment including cost and risk impact, back-out plans and Release Management plans for major changes	X	
9. Develop and maintain a schedule of planned changes and provide to the County for review	X	
10. Authorize and approve scheduled changes		X
11. Schedule and conduct Change and Release Management meetings to include review of planned changes and results of changes made	X	
12. Provide change documentation as required	X	
13. Coordinate notification of affected County clients of change timing and impact	X	
14. Implement change and adhere to detailed release plans	X	
15. Modify configuration database, asset management records, and service catalog (if applicable) to reflect changes implemented	X	
16. Verify that change met objectives, coordinate and resolve negative impacts	X	
17. Monitor changes and report results and impacts of changes	X	
18. Conduct User Acceptance Tests (UATs) as required		X
19. Perform Quality control audits and review change control results		X
20. Assist in Quality control audits	X	

Change and Release Management Roles and Responsibilities	Provider	County
21. Recommend procedures associated with County authorized Project Change Requests	X	
22. Review and approve the Project Change Request Process		X
23. Authorize change in project scope and design		X
24. Review maintenance production release plan and schedules		X
25. Manage all Service Requests to production		X
26. Ensure custom code approvals are received from the designated County IT personnel	X	
27. Assist the County with documentation and communicate change management processes and procedures	X	
28. Participate in scheduling releases	X	
29. Manage documentation changes to the underlying application development environment via use of library management version control and turnover management as described above	X	
30. Provide impact analysis associated with proposed project changes		X
31. Manage changes to the baseline, project plan, or committed maintenance or enhancement dates		X
32. Prepare County system change requests	X	
33. Approve system changes via the County Change Management Group		X

3.1.4.5 Account Management

Account Management services are the activities associated with the ongoing management of the service environment. The following table identifies Account Management roles and responsibilities that Provider and the County will perform.

Table 21. Account Management Roles and Responsibilities

Account Management Roles and Responsibilities	Provider	County
1. Define Account Management requirements and policies		X
2. Develop and document in the Procedures Manual Account Management procedures that meet requirements and adhere to defined policies	X	
3. Review and approve Account Management procedures		X
4. Develop a detailed "IT" service catalog which details services offered including all service options, pricing, installation timeframes, order process (new, change & remove service) and prerequisites	X	
5. Develop a service ordering process that clearly defines how to order, change, or delete services	X	
6. Recommend criteria and formats for Administrative, Service Activity and Service Level reporting	X	

Account Management Roles and Responsibilities	Provider	County
7. Review and approve criteria and formats for Administrative, Service Activity and Service Level reporting		X
8. Develop and implement Customer Satisfaction program for tracking the Quality of service delivery to End-Users		X
9. Provide reporting (e.g., statistics, trends, audits)	X	

3.1.4.6 Monitoring, Reporting and Review

Monitoring, Reporting and Review Services are the activities associated with the ongoing health checks, status reporting, and problem management (ongoing surveillance, tracking, escalation, resolution, and tracking of problems) of application support activities. Problem management activities described within this document require the Provider to provide Tier 2 technical support in coordination with the Help Desk.

The following table identifies the Monitoring, Reporting and Review roles and responsibilities that Provider and the County will perform.

Table 22. Monitoring, Reporting and Review Roles and Responsibilities

Monitoring, Reporting and Review Roles and Responsibilities	Provider	County
1. Provide, maintain and update project plans, identifying critical path dependencies, major critical milestones, project deliverables, "project earned value" as mutually agreed upon by the Parties for selected projects.		X
2. Provide weekly status reviews and progress reports for selected mutually agreed to projects	X	
3. Provide monthly service-level performance reports against each Service Level Agreement, including trends for each and summary view	X	
4. Provide monthly milestone achievement review and performance reports	X	
5. Provide mutually agreed to reports to enable invoice reconciliation	X	
6. Provide mutually agreed to reports that capture service requests demands and measure of ability to satisfy demand	X	
7. Provide mutually agreed reports that represent general health of environments as well as reports that represent demand fulfillment in End-User terms (e.g. defect corrections/change requests that have slipped against commitment, backlogged defects/change requests, Priority 1, 2, and Priority 3 defects).	X	
8. Measure and analyze performance relative to requirements	X	

3.2 Exclusions

The following items are specifically excluded from this statement of work:

- a. Data Communications/LAN/WAN
- b. Data Security
- c. Voice over IP
- d. Project Management
- e. Asset Control/Management

4.0 Service Management

4.1 Objectives

4.2 Definitions

Attachment A2 (SOW Definitions) of the Agreement provides a list of terms that apply to this SOW and the following Service Levels.

4.3 Service Level Requirements (SLRs)

The following service levels are suggested as commercially reasonable efforts. All times referenced are in Pacific Time.

Table 23. Incident Resolution SLRs

Definition

Time to resolve Incidents following responses to different Incident priority classifications.

Each IT Services Tower SOW categorizes Incidents according to the Incident Resolution Priorities listed below. Service Tower Incident categorizations are referenced in the Service Management section of each Service Tower SOW.

Incident Resolution SLRs			
Incident Resolution	Service Measure	Performance Target	SLR Performance %
Priority 1	Time to Resolve	<2 hours	98.0%
Priority 2	Time to Resolve	<4 hours	95.0%
Priority 3	Time to Resolve	<8 hours	95.0%
Priority 4	Time to Resolve	Next Business Day or as prioritized by the County	95.0%
Root Cause Analysis	Time to Report	Within 24 business hours of Incident Resolution	95.0%
	Formula	Number of requests completed within Performance Target/Total of all requests occurring during Measurement Interval	
	Measurement Interval	Measure Weekly	
	Reporting Period	Report Monthly	
	Measurement Tool	TBD	

Table 24. Priority Levels

Priority Level	Description
1 - Emergency/Urgent	<p>The Problem has caused a complete and immediate work stoppage affecting a primary business process or a broad group of users such as an entire department, floor, location, or external users. No work around available.</p> <p>Examples:</p> <ul style="list-style-type: none"> Major application Problem (e.g., IFAS, CLETS, etc.) Severe Problem during critical periods (e.g., Payroll cycle) Security Violation (e.g., denial of service, widespread virus, etc.) Problems effecting public safety systems assumed to be priority 1 unless determined otherwise.
2 - High	<p>A business process is affected in such a way that business functions are severely degraded, multiple users are impacted or a key user is affected. A Workaround may be available; however, the Workaround is not easily sustainable.</p> <p>Examples:</p> <ul style="list-style-type: none"> Major application (e.g., Exchange) Key users (e.g., Supervisors, Department Head)
3 - Medium	<p>A business process is affected in such a way that certain functions are unavailable to End-Users or a system and/or service is degraded. A Workaround may be available</p> <p>Examples:</p> <ul style="list-style-type: none"> Telecommunication Problem (e.g., Blackberry, PBX digital/analog card) Workstation Problem (e.g., hardware, Software)
4 - Low	<p>An Incident that has little impact on normal business processes and can be handled on a scheduled basis. A Workaround is available.</p> <p>Examples:</p> <ul style="list-style-type: none"> User requests (e.g., system enhancement) Peripheral Problems (e.g., network printer) Preventative Maintenance

4.3.1 Backup and Restore Requirements

Provider shall implement and maintain backup and restoration capabilities for all Service Tower data, applications and component configurations. Provider shall perform incremental backups, full backups and full archive backups according to the Backup Schedule presented below. Recovery procedures will be capable of restoring service delivery for failed Service Tower data, applications and component configurations according to the Cross Functional Restoration SLRs listed below. Service tower applications requiring scheduled backups are referenced in the Service Environment section of each Service Tower SOW.

Table 25. Backup Schedule

Backup Schedule and SLRs						
Type of Backup	Backup Frequency	Storage Site	Retention/Purge Period Standard		Target	SLR Performance %
Incremental	Daily	Off-site	35 days		Backup Frequency	99.9% (See NOTE 1)
	Database					

Backup Schedule and SLRs						
Type of Backup	Backup Frequency	Storage Site	Retention/Purge Period Standard		Target	SLR Performance %
Full (Backup)	Weekly	Off-site	5 weeks		Backup Frequency	99.9% (See NOTE 1)
Full (Archive)	Monthly	Off-site	Indefinite		Backup Frequency	99.9% (See NOTE 1)
All					Quarterly Test each type of backup	100%

NOTE 1: SLR Performance Requirement shall be 99.0% until an Enterprise Backup solution is implemented. At that time, the SLR Performance Requirement shall become 99.9% as indicated.

Table 26. Restoration SLR

Restoration Services Table			
Restoration Type	Service Measure	Performance Target	SLR Performance %
Restore Requests for production data	Response Time Data 1 week old or less	≤ 3 hours from County request	99.0% of the time
Restore Requests for recovery of test data or data volume back-ups	Response Time Data 1 week old or less	≤ 8 hours from County request	99.0% of the time
Restore Requests for recovery of data or data volume back-ups	> than 1 week old	Commence restore within 3 Business Days	99.0% of the time
Formula		Number of requests completed within Performance Target /Total of all requests occurring during Measurement Interval	
Measurement Interval		Measure Weekly	
Reporting Period		Report Monthly	
Measurement Tool		TBD	

4.4 Reports

Provider shall provide written reports to the County regarding Provider's compliance with the SLRs specified in this Section and other management reports. Reports are required per the following:

Table 27. Cross Functional Services Reports

Report Description	Timing
TBD	

5.0 List of Referenced MSA Schedules

SOW APPENDIX	DESCRIPTION
A.1	Solano Work in Progress
A.2	Solano Future Initiatives
MSA SCHEDULE	DESCRIPTION
Modified Schedule 2B	Data Center Services SOW
Modified Schedule 2C	Desktop Support Services SOW
Schedule 2D	Server Administration Services SOW
Modified Schedule 2E	Help Desk Services SOW
Modified Schedule 2F	Application Services SOW
Attachment A2	SOW Definitions



SCHEDULE 2D
MODIFIED DATA NETWORK SERVICES SOW
for
SOLANO COUNTY

March 14, 2006
Updated June 7, 2006
Updated May 19, 2014
Updated November 29, 2018

Table of Contents

1.0	Data Network Services Overview	1
2.0	Service Environment	1
2.1	Scope of Infrastructure to be Supported	1
2.2	Baseline Information.....	2
3.0	Data Network Services Requirements	3
3.1	Service Descriptions and Roles & Responsibilities	3
3.2	Exclusions	13
3.3	Documentation	14
3.4	Service Specific Milestones.....	14
4.0	Service Management	15
4.1	Objectives.....	15
4.2	Definitions.....	15
4.3	Service Level Requirements (SLRs)	15
4.4	Reports.....	19
5.0	Referenced SOW Appendices and SOW Schedules	19

List of Tables

Table 1.	Data Network Baseline Projections	2
Table 2.	General Roles and Responsibilities.....	4
Table 3.	Design and Engineering Roles and Responsibilities	5
Table 4.	Asset Acquisition and Network Provisioning Roles and Responsibilities	5
Table 5.	Data Network Operations and Administration Roles and Responsibilities	6
Table 6.	Data Network Monitoring and Reporting Roles and Responsibilities	7
Table 7.	Remote Access Services Roles and Responsibilities	8
Table 8.	Circuit Support Roles and Responsibilities.....	9
Table 9.	Collaborative Computing Roles and Responsibilities	10
Table 10.	Firewall Management / Internet Services Roles and Responsibilities	10
Table 11.	Security Intrusion Detection Services Roles and Responsibilities.....	12
Table 12.	Security Vulnerability & Penetration Services Roles and Responsibilities	12
Table 13.	Security Incident & Audit Management Roles and Responsibilities	13
Table 14.	Network Availability SLRs.....	16
Table 15.	Network Administration Services SLRs	17
Table 16.	Security Management SLRs.....	18
Table 17.	Network Service Reports.....	19

This is Schedule 2D (Data Network Services SOW) to the Agreement between Solano County ("County") and Provider. Unless otherwise expressly defined herein, the capitalized terms used herein shall have the meaning assigned to them in Attachment A2 (SOW Definitions) or in the Agreement.

1.0 Data Network Services Overview

This Schedule 2D (Data Network Services SOW) is the Statement of Work (or "SOW") that sets forth the roles and responsibilities of the Parties for the Data Network Services ("Data Network Services") provided under the Agreement as part of the Services. Data Network Services are the Services and activities, as further detailed in this SOW, required to provide and support the County's Data Network. Provider responsibilities include, but are not limited to, the provisioning, management, administration and troubleshooting of the following Data Network Services:

- Wide-area Network (WAN)
- Local-area Network (LAN)
- Virtual Private Network (VPN)
- Network Security
- Collaborative Computing
- Remote Access Services
- Network Management

In addition to the Services described in this Data Network Services SOW, Provider is responsible for providing the Services described in Schedule 2A – Cross Functional Services SOW.

2.0 Service Environment

2.1 Scope of Infrastructure to be Supported

The following sub-sections and related Service Environment Appendices further describe and scope the Data Network Services environment to be supported and/or with which Provider shall comply. These Service Environment Appendices are to be maintained by Provider, reviewed with the County, updated by Provider and made available to the County on a quarterly basis.

2.1.1 Network Hardware and Software

- A listing and description of all Network hardware to be provided and supported is provided in Appendix D.1 – Data Network Hardware.
- A listing and description of the Network software and utilities to be provided and supported is provided in Appendix D.2 – Data Network Software.
- A listing of Network circuits to be provided and supported is provided in Appendix D.3 – Data Network Circuits.
- A Network topology diagram describing the Network components to be provided and supported is provided in Appendix D.4 – Data Network Topology.

2.1.2 Server Hardware and Software

A listing of all Server hardware and Software will be in the following Data Center Appendixes:

- a. A listing and description of all Data Center hardware to be supported is provided in Appendix B.1 – Data Center Hardware.

A listing and description of the Systems Software and utilities to be supported is provided in Appendix B.2 – Data Center Systems Software.

2.1.3 Service Locations

A description and location of all the County facility and office locations requiring Data Network Services is provided in Appendix D.5 – County Service Locations.

2.1.4 Personnel

Provider will be responsible for providing appropriately skilled staffing to meet the Data Network Services Roles and Responsibilities and Service Levels set forth in this SOW.

2.1.5 Policies, Procedures and Standards

The policies, procedures and standards with which Data Network Services will comply are provided in Appendix D.6 – Data Network Policies, Procedures and Standards. *(To be proposed and developed with selected Provider)*

2.1.6 Agreements and Licenses

A list of Data Network related agreements and licenses to be supported are provided in Appendix D.7 – Data Network Agreements and Licenses.

2.2 Baseline Information

The County's current Network utilization and projected usage is presented below. These business requirements represent the County's most realistic projection of the Service requirements for Day 1 implementation based on a combination of past trends and current anticipated overall business direction over the term of the contract.

These metrics, along with other data which may be pertinent for sizing the solution, are reflected in Schedule 3 – Fees.

Table 1. Data Network Baseline Projections

System	Baseline	Yr 1	Yr 2	Yr 3	Yrs 4-5	Yrs 6-7	Comments
Routers	69	75	80	85	95	105	
DSCs/CSUs	59	65	70	75	85	95	
Switches	352	375	400	425	475	525	
Firewalls	8	11	14	17	23	30	
Fiber – 1GB	26	30	34	40	50	60	
ATM – 20MB	4	4	2	0	0	0	
T1 – 1.544MB	29	35	40	45	55	65	
Frame Relay – 1.544MB	4	4	4	2	0	0	

System	Baseline	Yr 1	Yr 2	Yr 3	Yrs 4-5	Yrs 6-7	Comments
56K Circuit	9	9	9	6	3	0	
ISDN – 128KB	1	1	1	0	0	0	
Modems/Modem Pool	3	3	3	3	3	3	
VPN - Accounts	282	312	342	372	400	430	
IMACs per device/per year	5	5	5	5	5	5	

3.0 Data Network Services Requirements

3.1 Service Descriptions and Roles & Responsibilities

In addition to the Services, activities, and roles and responsibilities described in Schedule 2A – Cross Functional Services SOW, Provider is responsible for the following Data Network Services.

3.1.1 Data Network Services

a. Wide Area Network (WAN) Services

WAN services include the provisioning, monitoring and management of networks that interconnect two or more separate facilities that span a geographic area larger than a campus or metropolitan area. Transmission facilities include, but are not limited to, point to point circuits, Frame Relay, dedicated Internet connections, broadband (DSL/Cable Modem) Internet connections, Internet-based VPNs, and dial-up connections. Provider shall work with public carriers and other County circuit providers on behalf of the County to ensure delivery of WAN services. Support of any network services-related work required by designated carriers, to support the County network, is considered within the scope of services.

Local Area Network (LAN) Services

LAN services include the provisioning and monitoring and management of networks that are usually confined to a single facility or portion of a facility. LAN components include Dynamic Host Control Protocol (DHCP)/Domain Name Server (DNS) and Wireless LANs supporting all network traffic originating from desktop devices, local file and print servers, application servers, database servers, peripherals, firewalls/routers, other network devices and other Premise Devices. This service ends at, but does not include the back of the Network Interface Card (NIC) on the desktop.

Virtual Private Network (VPN) Services

VPN services include the provisioning and monitoring and management of methods for remote users and business partners to securely connect to the Network and Data Center Computing Services over the public Internet. This service includes dedicated site-to-site VPN connectivity on a shared public IP network. It requires industry/Internet-based standards for Security to create and preserve privacy, data integrity, and authenticity. The VPN service must be highly scaleable.

Remote Access Services

Remote Access Services (RAS) include the provisioning and Monitoring and Management of a connection methodology for remote End-Users to securely connect to the Network and Data Center and Server Services. RAS may consist of a variety of technologies, including:

- Dial-up direct
- Dial-up through VAN Provider
- Dial-up through internet access Provider and VPN
- IPsec VPN access
- SSL VPN access
- Windows Terminal Service
- WEB mail

Network Security Services

Network Security Services includes the provisioning and support of methods that provide Security to physical and logical devices connected to the network. Security services include, but are not limited to Firewall, Intrusion Detection, Penetration/Vulnerability testing.

3.1.2 General Responsibilities

The following table identifies General roles and responsibilities associated with this SOW. An "X" is placed in the column under the Party that will be responsible for performing the task. Provider responsibilities are indicated in the column labeled "Provider."

Table 2. General Roles and Responsibilities

General Roles and Responsibilities	Provider	County
1. Recommend WAN / LAN/ VPN / Firewall requirements and standards based on industry best practices	X	
2. Review and approve requirements and standards for WAN/LAN/VPN/Firewall services		X
3. Recommend Network capacity thresholds plans	X	
4. Review and approve Network capacity thresholds plans		X
5. Provide Network capacity and performance reports	X	
6. Procure all Network components and circuits		X
7. Report performance against Service Level Requirements	X	
8. Support all infrastructure software computer-processing services (e.g. messaging, Internet, Intranet and Extranet)	X	
9. Manage End-User accounts, disk space quotas and access control	X	

3.1.3 Design and Engineering Services

Design and Engineering Services are the activities associated with the design and engineering of the technical infrastructure, tools and utilities to support the Data Network environment. The

following table identifies the Data Network Architecture, Design and Engineering roles and responsibilities that Provider and the County will perform.

Table 3. Design and Engineering Roles and Responsibilities

Design and Engineering Roles and Responsibilities	Provider	County
1. Prepare and provide Network design, engineering, security plans and schedules to support new and enhanced applications, architectures and standards based on established Procedures	X	
2. Review and approve Network design, engineering, security plans, and schedules		X
3. Develop and document in the Procedures Manual Network Design and Engineering procedures that meet requirements and adhere to defined policies	X	
4. Provide recommendations for optimizing Network design	X	
5. Review and approve recommendations for optimizing Network design		X
6. Develop scheduling of changes to the Network environment	X	
7. Review and approve the scheduling of changes to the Network environment.		X
8. Coordinate changes to the Network environment with the County and public carriers, as required for in-scope services	X	

3.1.4 Asset Acquisition and Network Provisioning

Asset Acquisition and Network Provisioning Services are the activities associated with the pricing, evaluation (technical and costing), selection, acquisition, and ongoing management and disposition of new and upgraded Network circuits and components. The following table identifies the Asset Acquisition and Network Provisioning roles and responsibilities that Provider and the County will perform.

Table 4. Asset Acquisition and Network Provisioning Roles and Responsibilities

Asset Acquisition and Network Provisioning Roles and Responsibilities	Provider	County
1. Recommend Asset Acquisition and Network Provisioning requirements and policies	X	
2. Review and approve Asset Acquisition and Network Provisioning requirements and policies		X
3. Develop and document in the Procedures Manual Asset Acquisition and Network Provisioning procedures that meet requirements and adhere to defined policies	X	
4. Review and approve Asset Acquisition and Network Provisioning procedures		X
5. Order and expedite WAN circuits, equipment and Services as defined by the County	X	
6. Configure WAN/LAN (hardware, Software) prior to installation	X	
7. Document router configuration files and IP addressing schemas	X	

Asset Acquisition and Network Provisioning Roles and Responsibilities	Provider	County
8. Coordinate ordering, procurement and inventory management of Network circuits from public carriers	X	
9. Manage the performance of public carriers (and other Third Parties) to meet defined schedules, project plans, SLRs, etc.	X	
10. Ensure that all new circuits, devices and Software provisioned are included in configuration management documentation	X	

3.1.5 Data Network Operations and Administration

Data Network Operations and Administration Services are the activities associated with the provisioning and day-to-day management of the Data Network environment.

a. Network Operations activities include:

- Network systems management and troubleshooting (e.g., performance, Incident, change and capacity monitoring);
- Bandwidth management;
- Protocol usage statistics (e.g., identify top talkers by protocol);
- Working with public carriers and other circuit providers to perform any operations activities (e.g., provisioning, Incident management); and
- Managing and maintaining all Data Network Service resources (e.g., hardware, Software, circuits) that are required to provide designated Services.

Network Administration Services include activities, such as:

- Managing router configurations, firewalls, Internet Protocol (IP) addresses and related Devices (e.g., DNS/DHCP)
- Asset management, including infrastructure software licenses
- Physical (e.g., equipment) and logical (e.g., IP address change) IMACs

The following table identifies the activities, roles and responsibilities associated with Data Network Operations and Administration that are specific to this Schedule.

Table 5. Data Network Operations and Administration Roles and Responsibilities

Data Network Operations and Administration Roles and Responsibilities	Provider	County
1. Recommend Data Network Operations and Administration requirements and policies	X	
2. Review and approve Data Network Operations and Administration requirements and policies		X
3. Develop and document in the Procedures Manual Data Network Operations and Administration procedures that meet requirements and adhere to defined policies	X	
4. Review and approve Data Network Operations and Administration procedures		X

Data Network Operations and Administration Roles and Responsibilities	Provider	County
5. Provide LAN/WAN connectivity contained in the service environment	X	
6. Perform day-to-day Network Operations and Network Administration activities	X	
7. Maintain Network devices operating systems software and firmware	X	
8. Manage secure file transfers, encryption and other secure data movement activities	X	
9. Manage all Network devices in accordance with the County's policies	X	
10. Maintain IP addressing schemes, router configurations, routing tables, VPN configurations, etc.	X	
11. Manage End-User accounts as needed for access and maintaining Network resources (e.g., logon End-User-id and password maintenance)	X	
12. Maintain and provide audit information including access, general logs, application logs in accordance with the County's Security policies	X	
13. Ensure that Network Administration activities are coordinated through defined change management and capacity management processes	X	

3.1.6 Data Network Monitoring and Reporting

Data Network Monitoring and Reporting are the activities associated with the monitoring and reporting of network performance and management information (e.g., performance metrics, Incidents). The following table identifies the Data Network Monitoring and Reporting roles and responsibilities that Provider and the County will perform.

Table 6. Data Network Monitoring and Reporting Roles and Responsibilities

Data Network Monitoring and Reporting Roles and Responsibilities	Provider	County
1. Recommend Data Network Monitoring and Reporting requirements and policies	X	
2. Review and approve Data Network Monitoring and Reporting requirements and policies		X
3. Develop and document in the Procedures Manual Data Network Monitoring and Reporting and Incident management procedures that meet requirements	X	
4. Review and approve Data Network Monitoring and Reporting and Incident management procedures		X
5. Recommend tools for monitoring Network devices and traffic	X	
6. Review, approve and provide tools for monitoring Network devices and traffic		X
7. Implement tools for monitoring Network devices and traffic	X	
8. Implement measures for proactive monitoring and self-healing capabilities to limit Network Outages	X	
9. Monitor Network per SLRs	X	

Data Network Monitoring and Reporting Roles and Responsibilities	Provider	County
10. Identify Network Incidents and Resolve in accordance to Incident Resolution policies, procedures and SLRs	X	
11. Provide on-site staff at County facilities as required to perform maintenance and Incident Resolution activities	X	
12. Monitor Network traffic to/from designated systems for current attack signatures and retained for 3 days	X	
13. Coordinate resolution of circuit Incidents with Third Parties, including public carriers, ISP and County affiliates using the Network	X	

3.1.7 Remote Access Services

Remote Access Services (RAS) are the activities associated with the provisioning and Monitoring and Management of a connection methodology for remote End-Users to securely connect to the Network and Data Center and Server Services. These activities include installation, management, operations, administration and support of the hardware and Software that supports Remote Access and connectivity to all systems (e.g., VPN, Extranet access, Citrix Metaframe via dial up and Internet, Web-based mail). The following table identifies the Remote Access Services roles and responsibilities that Provider and the County will perform.

Table 7. Remote Access Services Roles and Responsibilities

Remote Access Services Roles and Responsibilities	Provider	County
1. Recommend RAS requirements and policies, including security policies	X	
2. Review and approve RAS requirements and policies, including security policies		X
3. Develop, document and maintain in the Procedures Manual RAS Procedures that meet requirements and adhere to defined policies	X	
4. Review and approve RAS procedures		X
5. Install, test, provide technical support, administration and security administration for Remote Access hardware and software	X	
6. Provide testing support for defined County applications that will be made available via Remote Access	X	
7. Provide technical assistance and subject matter expertise as required by County infrastructure staff and third-party solution providers for remote access products and solutions	X	
8. Perform system or component configuration changes necessary to support Remote Access Services	X	

Remote Access Services Roles and Responsibilities	Provider	County
9. Manage RAS Services including: <ul style="list-style-type: none"> • Remote LAN access • Web portal / reverse proxy • Webmail • Windows terminal Server • SecureID • Dial in carriers Management • Other mutually agreed to services 	X	
10. Manage and maintain County's environment for RAS including: desktop firewalls and anti-virus deployment- supported in Desktop Services	X	

3.1.8 Circuit Support

Circuit Support is the activities associated with providing 24x7x365 support of the County global Network to ensure continuous operation. This support includes Problem isolation and determination to the Network Device port level. The following table identifies the Circuit Support roles and responsibilities that Provider and the County will perform.

Table 8. Circuit Support Roles and Responsibilities

Circuit Support Roles and Responsibilities	Provider	County
1. Recommend Circuit Support requirements and policies	X	
2. Review and approve Circuit Support requirements and policies		X
3. Develop, document and maintain in the Procedures Manual Circuit Support Procedures that meet requirements and adhere to defined policies	X	
4. Review and approve Circuit Support procedures		X
5. Isolate Problems to the Device level	X	
6. Contact the vendor as an agent and have the Device fixed or replaced as stated in the vendor maintenance contract if it is determined that a County owned Device is defective	X	
7. For circuit Incidents and Problems, contact carrier to determine the cause of the outage, notify County, and work on the Incident/Problem with carrier until Resolved	X	
8. Track Incidents and Problems, follow up on status, escalate when required and report to the appropriate Parties' status including when Incidents/Problems are Resolved	X	
9. Provide any possible Workarounds to help maintain production until a permanent fix can be achieved during Network Problems/outages	X	
10. Provide monthly reports on Network health, which shall include utilization graphs, protocol/application breakdown, top conversation lists, and top 20 high and low utilized circuits	X	
11. Meet with County to review pro-active WAN utilization	X	
12. Provide ad-hoc Network reports when requested	X	

3.1.9 Collaborative Computing

Collaborative Computing Services are the activities associated with the support of the existing and future collaborative tools (e.g. MS Exchange, Web mail, Net Meeting, SharePoint). These activities include the acquisition, installation, upgrades, maintenance, support and tuning of collaborative applications for optimal performance. The following table identifies the Collaborative Computing roles and responsibilities that Provider and the County will perform.

Table 9. Collaborative Computing Roles and Responsibilities

Collaborative Computing Roles and Responsibilities	Provider	County
1. Recommend Collaborative Computing requirements and policies for functions	X	
2. Review and approve Collaborative Computing requirements and policies for functions		X
3. Develop and document in the Procedures Manual Collaborative Computing procedures that meet requirements and adhere to defined policies	X	
4. Review and approve Collaborative Computing procedures		X
5. Install, test, provide technical support, database administration and security administration for Collaborative Computing applications	X	
6. Provide technical assistance and subject matter expertise support as required by County staff and Third-Party solution providers	X	
7. Provide Email archiving to meet regulatory and compliance requirements	X	

3.1.9.1 Firewall Management / Internet Services

Firewall Management / Internet Services are the activities associated with Managing and supporting County's firewalls, DMZ infrastructures, internet connections and Third Party connections. Provider shall provide Firewall Management / Internet Services including firewall engineering and Management and access control list engineering and Management in compliance with County's policies and Standards and Procedures Manual. Provider will maintain and operate the firewall/DMZ/Internet infrastructure in such a way that Services are secure and reliable and perform according to requirements and SLRs. Provider will also make recommendations on design Changes to improve Services as well as doing the implementations per the Change Management Procedures. On behalf of County, Provider will act as an agency to contact ISPs and/or other Third Parties to setup connectivity and/or troubleshoot connections and other support questions. Provider will perform filtering outbound internet browsing and keeping the tables for filtering up to date as well as tracking the usage licensing. The following table identifies the Firewall Management / Internet Services roles and responsibilities that Provider and the County will perform.

Table 10. Firewall Management / Internet Services Roles and Responsibilities

Firewall Management / Internet Services Roles and Responsibilities	Provider	County
1. Recommend industry best practices for Firewall Management	X	
2. Review and approve County specific Firewall Management policies and requirements		X

Firewall Management / Internet Services Roles and Responsibilities	Provider	County
3. Develop, document and maintain in the Procedure Manual all Firewall Management Procedures that meet requirements and adhere to defined policies	X	
4. Review and approve Firewall Management procedures		X
5. Provide Services in conformance to County firewall policies	X	
6. Perform firewall engineering and firewall Security design	X	
7. Assess firewall security and propose alternative Security designs	X	
8. Review and approve firewall Security designs		X
9. Design an infrastructure architecture that will allow secure web site access and authentication	X	
10. Review and approve infrastructure architecture and firewall security designs		X
11. Maintain configuration of web Servers	X	
12. Implement defined web access requirements and standards via firewall rule sets	X	
13. Ensure compliance to defined security and configuration standards including internet content filtering and data encryption	X	
14. Define intranet/Internet boundaries within the County		X
15. Assist with the definition of intranet/Internet boundaries within the County	X	
16. Maintain intranet/internet boundaries within the County	X	
17. Recommend Third Party connectivity strategy	X	
18. Review and define Third Party connectivity strategy		X
19. Support and Manage content compression devices, load balancing devices, and SSL acceleration	X	
20. Monitor performance levels of the firewall/DMZ/Internet infrastructure through setting of thresholds and take pro-active and/or re-active steps to Resolve any performance issues.	X	
21. Provide ongoing recommendations for improved Security	X	
22. Review and approve recommendations for improved Security		X
23. Define URL Filtering requirements		X
24. Manage URL Filtering Software to support County defined URL Filtering requirements	X	
25. Provide monthly and ad-hoc Internet usage reporting	X	

3.1.9.2 Security Intrusion Detection Services

Security Intrusion Detection Services are the activities associated with Network-based Intrusion Detection Service (NIDS), Host-based Intrusion Detection Service (HIDS), and Network / Host-

based Intrusion Prevention Services (HIDS/HIPS). The following table identifies the Security Intrusion Detection roles and responsibilities that Provider and the County will perform.

Table 11. Security Intrusion Detection Services Roles and Responsibilities

Security Intrusion Detection Services Roles and Responsibilities	Provider	County
1. Recommend Security Intrusion Detection requirements and policies	X	
2. Review and approve Security Intrusion Detection requirements and policies		X
3. Develop and document in the Procedures Manual Security Intrusion Detection procedures that meet requirements and adhere to defined policies	X	
4. Review and approve Security Intrusion Detection procedures		X
5. Provide Security Intrusion Detection Services and reporting	X	
6. Allow for independent Security Intrusion Detection Services	X	
7. Provide ongoing recommendations for improved Security	X	
8. Review and approve recommendations for improved Security		X
9. Implement approved recommendations for improved Security	X	

3.1.9.3 Security Vulnerability & Penetration Services

Security Vulnerability & Penetration Services are the activities associated with testing the susceptibility of the County's Networks to a specific attack or suite of attacks targeting all County Intranet address space using automated and custom methods. The following table identifies the Security Vulnerability and Penetration roles and responsibilities that Provider and the County will perform.

Table 12. Security Vulnerability & Penetration Services Roles and Responsibilities

Security Vulnerability & Penetration Services Roles and Responsibilities	Provider	County
1. Recommend Security Vulnerability & Penetration requirements and policies	X	
2. Review and approve Security Vulnerability & Penetration requirements and policies		X
3. Develop and document in the Procedures Manual Security Vulnerability & Penetration procedures that meet requirements and adhere to defined policies	X	
4. Review and approve Security Vulnerability & Penetration procedures		X
5. Conduct Security vulnerability scans & penetration testing	X	
6. Allow for independent vulnerability & penetration services	X	
7. Cooperate with third party for testing Security Vulnerability & Penetration	X	
8. Provide reporting on Security Vulnerability & Penetration testing results	X	
9. Provide ongoing recommendations for improved Security	X	

Security Vulnerability & Penetration Services Roles and Responsibilities	Provider	County
10. Review and approve recommendations for improved Security		X
11. Implement approved recommendations for improved Security	X	

3.1.9.4 Security Incident & Audit Management Services

Security Incident and Audit Management Services are the activities associated with maintaining requirements in connection with Security Incident & Audit Management Services. The following table identifies the Security Incident and Audit Management roles and responsibilities that Provider and the County will perform.

Table 13. Security Incident & Audit Management Roles and Responsibilities

Security Incident & Audit Management Services Roles and Responsibilities	Provider	County
1. Recommend Security Incident and Audit Management requirements and policies	X	
2. Review and approve Security Incident and Audit Management requirements and policies		X
3. Develop and document in the Procedures Manual Security Incident and Audit Management procedures that meet requirements and adhere to defined policies	X	
4. Review and approve Security Incident and Audit Management procedures		X
5. Provide initial review (Priority Level 1) of Security Incidents and the determination if escalation to the County Information Security (Priority Levels 2, 3 support) is warranted	X	
6. Identify and remove from the Network any PC virus/worm infected system	X	
7. Identify and provide countermeasures for virus / worm attacks	X	
8. Establish Security audit policies		X
9. Conduct security audits		X
10. Provide support for Security audits	X	
11. Collect and review all Incidents reported by all other Security services (e.g., NIDS, HIDS, penetration testing, firewall).	X	
12. Maintain a central repository of log files in accordance with County policies and service levels including application-specific and system-specific log files	X	
13. Provide Security reporting	X	

3.2 Exclusions

The following items are specifically excluded from this statement of work:

- a. None at this time.

3.3 Documentation

In addition to the Services, activities, and roles and responsibilities described in this section, Provider is responsible for developing, revising, maintaining, reproducing, and distributing Data Network Infrastructure information in hard copy and electronic form. Some of the document types specific to this SOW include but are not limited to:

- a. Network system Specifications and topologies (e.g., router configurations, firewall policies, routing diagrams/IP addressing tables, hardware/Software listings)
- b. Detailed circuit location information (e.g., circuit ID including LEC access ID, location, speed)
- c. Firewall policies, group and object information
- d. "As-built" documentation for all Network devices (including firewalls) that are deployed in development, test, QA, production and other technical environments.
- e. Network diagram and information that complies with California DOJ requirements

3.4 Service Specific Milestones

Milestones specific to the deployment of Data Network Services are listed in the following:

Milestone Description	Milestone Date
TBD	

4.0 Service Management

4.1 Objectives

A key objective of the Agreement is to attain service levels with Fee Reductions where business is impacted through failure to meet Service performance requirements, mission critical system requirements or meet Critical Milestones or objectives. SLRs are detailed in the following sections and those associated with Fee Reductions are identified in Schedule 4 - Fee Reductions.

Provider shall provide written reports to the County regarding Provider's compliance with the SLRs specified in this SOW.

4.2 Definitions

Attachment A2— SOW Definitions of the Agreement provides a list of terms that apply to this SOW and following SLRs.

4.3 Service Level Requirements (SLRs)

The following minimum service levels are required at the end of the Transition Period. Provider must consistently meet or exceed the following SLRs. SLRs associated with Fee Reductions are detailed in Schedule 4 - Fee Reductions. All times referenced are in Pacific Time.

Table 14. Network Availability SLRs

DEFINITION	<p>Network Availability is defined as the time during which the Network is fully functioning as specified below and normal business operations can be carried out with no data loss, downtime, or performance degradation.</p> <p>All performance criteria are to be measured on a <i>per circuit and component basis</i> – criteria are <i>not</i> to be aggregated and averaged for all circuits and Network components.</p>
PRE-SCHEDULED DOWNTIME REQUIREMENTS	<p>All activities for downtime must be scheduled. There will not be any pre-scheduled maintenance period.</p>

Network Availability SLRs			
Service Type	Service Measure	Performance Target	SLR Performance %
Circuit Availability	Availability	7x24x365	99.99%
Internet Access Availability	Availability	7x24x365	99.9%
Network Hardware	Availability	7x24x365	99.9 %
LAN/WAN Availability	Availability	7x24x365	99.8%
VPN Availability	Availability	7x24x365	99.8 %
RAS Availability	Availability	7x24x365	99.8 %
	Formula	<p>Availability (%) = 100% - Unavailability (%)</p> <p>Where Unavailability is defined as:</p> $(\Sigma \text{ Outage Duration} \times 100\%) \div (\text{Schedule Time} - \text{Planned Outage})$	
	Measurement Interval	Monitor Continuously, Measure Daily, Report Monthly	
	Measurement Tool	TBD	

Table 15. Network Administration Services SLRs

DEFINITION	SLRs for Provider administration tasks to ensure Network Administration Services occur timely, to minimize capacity bottlenecks, and to maintain and improve operational usage and user access. Measurements for these services are 24x7x365 requirement.		
Network Administration Services SLRs			
Administration Task	Service Measure	Performance Target	SLR Performance %
Network Service capacity	Proactive monitoring and preemptive intervention to advise County of need to increase capacity	Network utilization reaches 60% of capacity	
Notification of vendor software and firmware patches, upgrades and new releases	Response Time	Within 7 days after software vendor announcement	
Implementation of Service packs and updates to "dot" releases	Response Time	Within 30 days after approval by the County	
Implementation of version or major release updates	Response Time	Within 60 days after approval by the County	
New End-User Account (up to 5 per request)	Elapsed time	Completed within 1 Business Day of authorized request	99.0%
New End-User Account (6-20 per request)	Elapsed time	Completed within 2 Business Days of authorized request	99.0%
New End-User Account (20+ per request)	Elapsed time	Case by case	N/A
Terminate End-User Account	Elapsed time	After 14 Business Days of authorized request	99.9%
	Formula	Transactions completed within Performance Target / Total Transactions	
	Measurement Interval	Monitor Continuously, Measure Daily, Report Monthly	
	Measurement Tool	TBD	

Table 16. Security Management SLRs

DEFINITION	SLRs for Provider security tasks for proactive security monitoring and management to maintain and improve network security, performance and reliability. Measurements for this service are 7x24x365 requirement.		
Security Management SLRs			
Management Task	Service Measure	Performance Target	SLR Performance %
Service/Security patches and Antivirus updates	Elapsed Time to Update to target population for each deployment	<= 1 calendar day Measured from approval for deployment by the County to successful deployment for End-Users who connect to the Network during the specified time frame	99.9%
Firewall Management Implementation of firewall changes related to changing, adding/deleting firewall rules	Response Time	Emergencies: ≤2 hours Standard Requests: within normal change control parameters after submission by County	99.0%
Monitor for current attack signatures	Overall Schedule	Sun-Sat, 0000-2400	
Monitor for changes to selected local files	Overall Schedule	Sun-Sat, 0000-2400	
Review all Priority Level 1 and Priority Level 2 alerts and notify County	Elapsed Time	<15 minutes	99.9%
	Formula	Performance = Transactions completed per Management Task within Performance Target / Total Transactions per Management Task occurring during the Measurement Interval	
	Measurement Interval	Monitor Continuously, Measure Daily, Report Monthly	
	Measurement Tool	TBD	

4.4 Reports

Provider shall provide written reports to the County regarding Provider's compliance with the SLRs in addition to the reports specified in this Section. Reports are required per the following:

Table 17. Network Service Reports

REPORT DESCRIPTION	TIMING
TBD	

5.0 Referenced SOW Appendices and SOW Schedules

SOW Appendix	Description
B.1	Data Center Hardware
B.2	Data Center Systems Software
D.1	Data Network Hardware
D.2	Data Network Software
D.3	Data Network Circuits
D.4	Data Network Topology
D.5	County Service Locations
D.6	Data Network Policies, Procedures and Standards
D.7	Data Network Agreements and Licenses
MSA Schedule	Description
Schedule 2A	Cross Functional Services SOW
Schedule 3	Fees
Schedule 4	Fee Reductions
Attachment A2	SOW Definitions