pGc Paul Garstki Consulting

INDEPENDENT REVIEW

OF A PROPOSED

ENTERPRISE VOIP PROJECT

For the
State of Vermont
Agency of Digital Services (ADS)

Submitted to the
State of Vermont, Office of the CIO
by:

Paul E. Garstki, JD, Consultant
d/b/a/ Paul Garstki Consulting
344 Laird Pond Rd.
Plainfield, VT 05667
paulg.consulting@gmail.com

June 21, 2021

version 1.2a

TABLE OF CONTENTS

CONTENTS

1 Executive Summary 8

1.1 Cost Summary 8

1.2 Disposition of Independent Review Deliverables 9

1.3 Identified High Impact &/or High Likelihood of Occurrence Risks 10

1.4 Other Key Issues 11

1.5 Recommendation 11

1.6 Independent Reviewer Certification 11

1.7 Report Acceptance 11

2 Scope of this Independent Review 12

2.1 In-Scope 12

2.1.1 The Agency shall obtain independent expert review of any new information technology projects with a total cost of $1,000,000.00 or greater or when required by the Chief Information Officer 12

2.1.2 The independent review report includes: 12

2.2 Out-of-scope 12

3 Sources of Information 13

3.1 Independent Review Participants 13

3.2 Independent Review Documentation 13

4 Project Information 15

4.1 Historical Background 15

4.2 Project Goal 16

4.3 Project Scope 17

4.3.1 In-Scope 17

4.3.2 Out-of-scope 17

4.3.3 Major Deliverables 17

4.4 Project Phases, Milestones, and Schedule 18

5 Acquisition Cost Assessment 19

5.1 Cost Validation: 19

- **Professional Services cost represents contractual agreement with this consultant.** 20

5.2 Cost Comparison: 20

How do the above Acquisition Costs compare with others who have purchased similar solutions (i.e., is the State paying more, less or about the same)? 20

5.3 Cost Assessment: 21

6 Technology Architecture Review 22

6.1 State's Enterprise Architecture Guiding Principles 26

6.1.1 A. Assess how well the technology solution aligns with the business direction 26

6.1.2 B. Assess how well the technology solution maximizes benefits for the state 26

6.1.3 C. Assess how well the information architecture of the technology solution adheres to the principle of information is an asset 26

6.1.4 D. Assess if the technology solution will optimize process 26

6.1.5 E. Assess how well the technology solution supports resilience-driven security. 26

6.2 Sustainability 27

6.3 How does the solution comply with the ADS Strategic Goals enumerated in the ADS Strategic Plan of January 2020? 27

6.3.1 A. Leverage successes of others, learning best practices from outside Vermont. 27

6.3.2 B. Leverage shared services and cloud-based it, taking advantage of IT economies of scale. 27

6.3.3 C. Adapt the Vermont workforce to the evolving needs of State government. 27

6.3.4 D. Apply enterprise architecture principles to drive digital transformation based on business needs. 28

6.3.5 E. Couple IT with business process optimization, to improve overall productivity and customer service. 28

6.3.6 F. Optimize IT investments via sound project management. 28

6.3.7 G. Manage data commensurate with risk. 28

6.3.8 H. Incorporate metrics to measure outcomes. 28

6.4 Compliance with the Section 508 Amendment to the Rehabilitation Act of 1973, as amended in 1998 29

6.5 Disaster Recovery........ 29

6.6 Data Retention 30

6.7 Service Level Agreement........ 30

6.7.1 What are the post implementation services and service levels required by the state? 30

6.7.2 Is the vendor proposed service level agreement adequate to meet those needs in your judgment? 30

6.8 System Integration 31

6.8.1 Is the data export reporting capability of the proposed solution consumable by the State? 31

6.8.2 What data is exchanged and what systems (State and non-State) will the solution integrate/interface with?........ 31

7 Assessment of Implementation Plan 33

7.1 The reality of the implementation timetable 33

7.2 Readiness of impacted divisions/ departments to participate in this solution/project 33

7.3 Do the milestones and deliverables proposed by the vendor provide enough detail to hold them accountable for meeting the Business needs in these areas: 34

7.3.1 A. Project Management 34

7.3.2 B. Training 34

7.3.3 C. Testing........ 34

7.3.4 D. Design 35

7.3.5 E. Conversion (if applicable)........ 35

7.3.6 F. Implementation planning 35

7.3.7 G. Implementation 35

7.4 Does the State have a resource lined up to be the Project Manager on the project? If so, does this person possess the skills and experience to be successful in this role in your judgment? 36

8 Cost Analysis and Model for Benefit Analysis 38

8.1 Analysis Description: 38

8.2 Assumptions: 38

8.3 Funding: 38

8.4 Tangible Costs & Benefits: 38

8.5 Intangible Costs & Benefits: 39

8.6 Costs vs. Benefits: 39

8.7 IT ABC Form Review: 40

9 Analysis of Alternatives 41

9.1 Provide a brief analysis of alternate technical solutions that were deemed financially unfeasible. 41

9.2 Provide a brief analysis of alternate technical solutions that were deemed unsustainable. 41

9.3 Provide a brief analysis of alternate technical solutions where the costs for operations and maintenance were unfeasible. 42

10 Impact Analysis on Net Operating Costs 43

10.1 Insert a table to illustrate the Net Operating Cost Impact. 43

10.2 Provide a narrative summary of the analysis conducted and include a list of any assumptions. 44

10.3 Explain any net operating increases that will be covered by federal funding. Will this funding cover the entire lifecycle? If not, please provide the breakouts by year. 44

10.4 What is the break-even point for this IT Activity (considering implementation and on-going operating costs)? 45

11 Security Assessment 46

11.1 Will the new system have its own information security controls, rely on the State's controls, or incorporate both? 46

11.2 What method does the system use for data classification? 46

11.3 What is the vendor's breach notification and incident response process? 47

11.4 Does the vendor have a risk management program that specifically addresses information security risks? 48

11.5 What encryption controls/technologies does the system use to protect data at rest and in transit? 48

11.6 What format does the vendor use for continuous vulnerability management, what process is used for remediation, and how do they report vulnerabilities to customers? 48

11.7 How does the vendor determine their compliance model and how is their compliance assessed? 49

12 Risk Assessment & Risk Register 50

12.1.1 Additional Comments on Risk 50

12.1.2 Risk Register 50

13 Attachments 56

13.1 Attachment 1 – Risk Register 57

13.2 Attachment 2 – Cost Spreadsheet 58

TABLES

Table 1 - Cost Summary 8

Table 2 - Disposition of Independent Review Deliverables 9

Table 3 - Identified High Impact &/or High Likelihood of Occurrence Risks 10

Table 4 - Independent Review Participants 13

Table 5 - Independent Review Documents 13

Table 6 - Major Deliverables 17

Table 7 - Project Milestones 18

Table 8 - Acquisition Costs 19

Table 9 - Net Operating Cost Impact 43

1 EXECUTIVE SUMMARY

Provide an introduction that includes a brief overview of the technology project and selected vendor(s) as well as any significant findings or conclusions. Ensure any significant findings or conclusions are supported by data in the report.

The proposed project will continue operation of the State's enterprise Voice over Internet Protocol (VoIP) system, which serves over 6,500 State employees at numerous Agencies and Departments. Importantly, it will also bring the system into compliance with the new Vermont e911 (enhanced 911) rule, which came into effect on July 1, 2019. The existing system has e911 capabilities but the new rule, as well as new federal law, requires the technological provision of information that very precisely identifies the caller's location. Other components of the project migrate users from the Department of Public Safety to the platform (they currently employ a different VoIP provider), enhance State management and reporting capabilities, and move internal State billing to the vendor.

The selected vendor is the incumbent vendor, NWN Corporation, which has a 6-year history of successful performance with the State, having implemented and operated the system.

Our review of the project indicates a likely cost savings to the State of $1,383,657, while increasing public and employee safety, ensuring e911 compliance, and enhancing function of the system as a whole.

1.1 COST SUMMARY

Table 1 - Cost Summary

IT Activity Lifecycle:	**5**
Total Lifecycle Costs:	**$6,442,752.84**
Total Implementation Costs:	**$471,763.89**
New Annual Operating Costs:	**$1,194,197.79**
Current Annual Operating Costs:	**$1,565,282.01**
Difference Between Current and New Operating Costs:	**$(371,084.22)**
Funding Source(s) and Percentage Breakdown if Multiple Sources:	**State**

1.2 DISPOSITION OF INDEPENDENT REVIEW DELIVERABLES

Table 2 - Disposition of Independent Review Deliverables

Deliverable	Highlights from the Review *Include explanations of any significant concerns*
Acquisition Cost Assessment	Acquisition cost for the project is $ 471,763.89. This is a relatively low figure compared to the approximately $1.2million annual operating cost because the project largely maintains operation of the current system, although at reduced cost. The implementation cost is largely the e911 compliance and DPS migration cost. The calculated cost per-user/per-month for the system, including State personnel costs, is $16.95, slightly lower but approximately in line with other cloud-based providers. Furthermore, that cost may be reduced even more if the State expands the user base, because State management costs are not likely to increase significantly.
Technology Architecture Review	The proposed system architecture is robust, reliable, state-of-the-art, and resilient. It is compliant in multiple ways with the State's IT strategic plan and it aligns closely with principles of Enterprise Architecture. It enhances the State's remote worker capabilities, supporting potential scenarios in the wake of the pandemic, and ensures e911 compliance even to remote workers. The State is protected in contract by a good Service Level Agreement, well-detailed and providing remedies in the event of missed service targets.
Implementation Plan Assessment	The main system is already in place, so we assessed the implementation plan for e911 compliance implementation. The vendor has a strong project management approach, and description of deliverables, vendor responsibilities, and State responsibilities speaks to a good grasp of project planning and a likelihood of keeping to the timeline.
Cost Analysis and Model for Benefit Analysis	We calculate a cost savings of **$1,383,657.21** over the lifecycle of the project, while enhancing capabilities. Intangible benefits include: • Full e911 rule and federal law compliance for the VoIP system, increasing employee and public safety, decreasing State liability, and enhancing State reputation. • Customer Service Improvement • Standardization of remote soft phone client, increasing reliability and security and decreasing support requirements, to increase flexibility for remote working.

Impact Analysis on Net Operating Costs	Annual operating costs for the proposed project are lower than those for the existing system. Combined with a low implementation cost, we expect that compared with projecting current operating costs over the 5-year lifecycle, breakeven point will be in the first year of operation.
Analysis of Alternatives	Given the State's stated preference for cloud-based, scalable systems, there are few technological alternatives that would not closely resemble the chosen system. Some alternative vendors' proposals were financially unfeasible.
Security Assessment	The vendor's security stance is extensive, well-supported, and meets the State's requirements and preferences in all ways. The vendor's stated security policies assure the State of compliance with data protection compliance across a variety of data classifications.

1.3 IDENTIFIED HIGH IMPACT &/OR HIGH LIKELIHOOD OF OCCURRENCE RISKS

NOTE: Throughout the narrative text of this document, **Risks and Issues are identified by bold red text**, and an accompanying tag (**_RISK_ID# _0_** provides the Risk or Issue ID to reference the risk, response, and reference in the Risk Register.

The following table lists the risks identified as having high impact and/or high likelihood (probability) of occurrence.

Please see the **Risk & Issues Register, in Section 10**, for details.

Table 3 - Identified High Impact &/or High Likelihood of Occurrence Risks

Risk Description	RATING IMPACT/ PROB	State's Planned Risk Response	Reviewer's Assessment of Planned Response
The State intends an increased and continuing reliance on softphone clients, instead of acquiring many more standalone phones. Softphones may pose an inherently greater potential security risk, compared to standalone phones, when they are deployed on workstations that have access to other network resources. (see, for example, https://www.cisco.com/c/en/us/support/docs/csa/cisco-sa-jabber-ttcgB9R3.html).	**30** **10 / 3**	**State agrees with reviewer to mitigate by working with vendor, establishing best practices for softphone clients.**	**concur**

However, they are very inexpensive, are in wide use, meet many State needs, and most established clients such as Cisco are monitored for vulnerabilities.

1.4 OTHER KEY ISSUES

none

1.5 RECOMMENDATION

We recommend that the project proceed as planned.

1.6 INDEPENDENT REVIEWER CERTIFICATION

I certify that this Independent Review Report is an independent and unbiased assessment of the proposed solution's acquisition costs, technical architecture, implementation plan, cost-benefit analysis, and impact on net operating costs, based on the information made available to me by the State.

E-SIGNED by Paul Garstki
on 2021-06-22 11:56:33 GMT

______________________________ ____________________

Independent Reviewer Signature **Date**

1.7 REPORT ACCEPTANCE

The electronic signatures below represent the acceptance of this document as the final completed Independent Review Report.

E-SIGNED by Morgan Amell
on 2021-06-22 11:59:16 GMT

______________________________ ____________________

ADS Oversight Project Manager **Date**

E-SIGNED by John Quinn
on 2021-06-22 13:17:04 GMT

______________________________ ____________________

State of Vermont Chief Information Officer **Date**

2 SCOPE OF THIS INDEPENDENT REVIEW

2.1 IN-SCOPE

The scope of this document is fulfilling the requirements of Vermont Statute, Title 3, Chapter 056, §3303(d):

2.1.1 THE AGENCY SHALL OBTAIN INDEPENDENT EXPERT REVIEW OF ANY NEW INFORMATION TECHNOLOGY PROJECTS WITH A TOTAL COST OF $1,000,000.00 OR GREATER OR WHEN REQUIRED BY THE CHIEF INFORMATION OFFICER

2.1.2 THE INDEPENDENT REVIEW REPORT INCLUDES:

A. An acquisition cost assessment;

B. A technology architecture and standards review;

C. An implementation plan assessment;

D. A cost analysis and model for benefit analysis;

E. An analysis of alternatives;

F. An impact analysis on net operating costs for the Agency carrying out the activity; and

G. A security assessment.

2.2 OUT-OF-SCOPE

- A separate deliverable contracted as part of this Independent Review may be procurement negotiation advisory services, but documentation related to those services are not part of this report.

3 SOURCES OF INFORMATION

3.1 INDEPENDENT REVIEW PARTICIPANTS

Table 4 - Independent Review Participants

Name	First interview	Employer and Title	Participation Topic(s)
Hunter Thompson	11/20/2020	ADS, IT Director	Project overall
Angela Leclerc	11/20/2020	ADS, Deputy Director	Project overall and finance
Leslie Baker	5/13/2021	ADS,	Project overall
Frank Costantino	5/13/2021	ADS, Telecommunications Director	Technical view of vendor, vendor experience
Troy Morton	11/20/2020	ADS, Enterprise Architect	Enterprise Architecture
David Kaiser	11/23/2020	ADS, Security Analyst	Security/Privacy
Cheryl Burcham	11/3/2020	ADS, Project Manager	Project Management
Morgan Amell	11/3/2020	ADS, Portfolio Manager	Project Oversight

3.2 INDEPENDENT REVIEW DOCUMENTATION

The following documents were used in the process and preparation of this Independent Review.

Table 5 - Independent Review Documents

Document	Source
IT Activity Business Case & Cost Analysis (IT ABC Form), Enterprise VoIP Comm Solution	State
Enterprise Voice-over-Internet-Protocol (VoIP) Project Project Charter	State
RFP for Enterprise Voice Over Internet Protocol Communications Solution	State

The State of Vermont Enterprise VoIP Communications Solution Proposal Response	NWN
Vermont VoIP – Executive Summary	NWN
Vermont VoIP – Milestones	NWN
ADS Enterprise VoIP Vendor Proposal Rating	State
Architecture Assessment VoIP Solution FINAL presentation	State
Bids Received.xlsx	State
2021_04_16 ADS Enterprise VoIP NWN Contract Draft	State
NWN Financial	NWN
NWN Presentation for Enterprise VoIP Final	NWN
NWN Financial	NWN
NWN Road Map	NWN

4 PROJECT INFORMATION

4.1 HISTORICAL BACKGROUND

In 2015, the Department of Innovation and Information (DII) initiated the State government's first large-scale Voice over Internet Protocol (VoIP) system to replace the legacy phone system, which relied on a multiplicity of Centrex landlines, office telephones, and fax machines, etc. The State contracted with vendor NWN of Waltham, Massachusetts to design and deploy the system. The State experienced generally high satisfaction with the system and the vendor over several years. In 2019, as a contract was nearing expiration, the Agency of Digital Services (ADS) Shared Services put forth a business case for issuing a Request for Proposals (RFP) for a state-wide, cloud-hosted governmental VoIP system with the aims of (1) lowering cost; (2) bringing the system into compliance with the new e911 rule; and (3) potentially expanding the user base. This proposed project was approved to begin procurement.

The existing VoIP system had e911 capabilities but was no longer compliant with the new State e911 rule (and later, also federal law), which requires all phones calling 911 to automatically send dispatch location information (precisely identifying the caller's location at a quite granular level, e.g., building floor and office) and provision of a Location Information Server (LIS) used to identify phone location by phone number.

Additionally, the State wished to gain better reporting capability on the use of the system. The State internally bills Agencies and Departments or other entities for their use of the system, and this billing is currently performed by State personnel, with some data limitations. It was hoped to improve this process with improved reporting or possibly to have a vendor conduct billing (but not collections).

The resulting RFP (issued November 9, 2019) began:

> *The Office of Purchasing & Contracting on behalf of the Vermont Agency of Digital Services (the State) is soliciting competitive sealed, fixed price proposals (Proposals) for a Cloud Hosted Voice-over-Internet-Protocol (VoIP) solution for the State (the Work) from qualified Contractors.*

and contained a Scope of Work (SOW) which was introduced with the statement:

> *The State of Vermont is interested in obtaining bids to meet the following business need(s):*
>
> *Selection of a Contractor to maintain and support an Enterprise-wide IP telephony platform reaching across all areas of local government. The State has an existing hosted VoIP environment. The State has made an investment in Cisco devices (models listed below). The current hosted environment is managed by Cisco Call Manager. The new solution must integrate with existing devices. There may be opportunity to enhance communications and collaboration. There may be further opportunities to migrate existing Centrex sites that were not migrated to the current VoIP platform. In addition, we are seeking call center integration for our existing platform.*

The RFP continued with a very detailed SOW and a description of the State's current environment, including equipment used, number of phones, locations, etc. The State required a proposed system to use existing State IP phone equipment to the greatest extent possible, avoiding the need for a capital equipment expenditure. The State wished to use its existing Cisco Call Manager infrastructure, with which it had significant experience and expertise, as well as capital investment. Functional and non-functional requirements were detailed, and bidders were also invited to bid on a number of options, in particular the integration or replacement of the State's existing Call Centers, as well as a migration of the phones of the Department of Public Safety (DPS), which uses a different VoIP platform, and the Department of Corrections.

The State received bids from 11 vendors, and the project team scored the proposals on a variety of qualifications and separately on price, and this procurement process resulted in the selection of 3 "semi-final" candidates, who were invited to make "demo" presentations to the procurement team. From this process 2 final candidates were selected, and the highest scoring, CBTS, was selected to begin contract negotiations. These negotiations continued for some weeks, but eventually the procurement team concluded that the vendor was unwilling or unable to comply fully with the State's needs and requirements. These negotiations were ended, and the State selected its second highest scoring finalist, NWN, who is also the incumbent vendor. We note that both vendors scored highly in the scoring process and were deemed acceptable by the Enterprise Architecture team at ADS.

The proposed project will

- Continue the existing VoIP system.
- Bring the system into compliance with the e911 rule.
- Expand service to the Department of Public Safety
- Expand reporting capabilities via the vendor's online management portal.
- Migrate billing processes to the vendor.

Additionally, the contract contains vendor pricing for migrating the State's contact centers as an option for a future project.

4.2 PROJECT GOAL

The State of Vermont seeks to achieve the following Business Value(s):

- Cost Savings: State is "hoping" to leverage cost savings.
- Compliance: New E911 Rule passed. Need to bring VoIP system into compliance with the new rule.
- Customer Service Improvement
  - Improved reporting capabilities – more flexibility to run reports needed for billing.
    - Long Distance call detail
    - Call detail – when requested – ideally users could query this on a self-service portal.

    - Billing Code information accuracy
  - Improved customer service – improved accuracy of moves/adds/changes/deletes.

4.3 PROJECT SCOPE

4.3.1 IN-SCOPE

- Integration with existing VoIP devices, utilized to manage phone models listed in the RFP. Cisco phones already purchased must be managed and supported by the new platform – model numbers listed in the RFP.
- Must adhere to E911 Rule for Enterprise Communications Systems. Enterprise Communication Systems (ECS) - Effective July 1st, 2019.
- The State's Functional and Non-Functional Requirements are provided in the attached State of Vermont Bidder Response Form (Exhibit C of the RFP).
- State will maintain voice/data network readiness, traffic capacity and on-going reliability from the demarcation points with Contractor's service to end-users.

4.3.2 OUT-OF-SCOPE

- Anything not explicitly in scope.
- Locations not included in the deployment plan.
- Network infrastructure investments beyond the scope of the VoIP project
- Agency/Department specific enhancements beyond current service level

4.3.3 MAJOR DELIVERABLES

Table 6 - Major Deliverables

The following are deliverables for the e911 compliance enhancement implementation.

Emergency Responder
Add switches
Add the location of the switch port
Add DIDs for Emergency Responder ELINs
Add ERLs
Add ELINs
Configure Notifications to State distribution lists as specified
Communications Manager

Add unique DIDs (1 per phone)
Add DIDs to the SIP Session Border Controllers (SBCs)
Add ERL translation patterns
Bandwidth.com
Add DIDs
Update ALI database

4.4 PROJECT PHASES, MILESTONES, AND SCHEDULE

Table 7 - Project Milestones

The following table lists project milestones for e911 enhancement implementation.

Phase	Estimated TIMEFRAME	Phase Description
Initiation	E911: 10 days	Kick-off meeting, Planning and preparation of project management planning documentation.
Requirements Gathering	E911: 10 days	Contractor performs necessary requirements gathering to finalize functional and technical requirements and identify gaps between State requirements and Solution capabilities.
Implementation	E911: 30 days	Contractor installs and configures the Solution in a Test environment.
Testing	E911: 30 days	State subject matter experts perform Solution testing in in a test (not live) environment accordance with Contractor-developed Test plans.
Training	E911: 10 days	Contractor performs training of State personnel (train the trainer or train the user).
Legacy Data Migration	E911: N/A	E911 Implementation will not require migrating legacy data
Deployment	E911: 20 days	Contractor implements the tested and State-approved Solution in the production environment for additional State testing and Go-Live.
Post-Implementation Support/Warranty	E911: Duration of contract term	Contractor shall be responsible for fixing all Defects found during the Warranty Period. All Defects found within the Warranty Period, shall be corrected by Contractor at no additional cost to the State.

5 ACQUISITION COST ASSESSMENT

This project primarily consists of a cloud-based Software-as-a-Service (SaaS) deployment. Since the State be paying for the service provided, and acquiring the vendor's platform supporting the service, the acquisition costs are a relatively small portion of the total lifecycle costs of the service provided. The required table below shows only acquisition costs, but we will consider lifecycle costs as well in the text following.

Table 8 - Acquisition Costs

Acquisition Costs	Cost	Comments
Hardware Costs	**$ 0**	*No hardware costs to State*
Software Costs	**$ 0**	*No software costs to State (note EMP platform migration in implementation services)*
Implementation Services	**$ 52,905.89**	
State Personnel	**$ 393,876.00**	*See attach. 3, Cost Spreadsheet*
Professional Services (e.g., Project Management, Technical, Training, etc.)	**$ 24,982.00**	*provided by IR consultant*
Total Acquisition Costs	**$ 471,763.89**	

5.1 COST VALIDATION:

Describe how you validated the Acquisition Costs.

Note that some of these costs are not acquisition (implementation) costs, and do not show in the above table. However, they are used in the Cost Summary shown in Section 1.1, above, and in the Cost Spreadsheet, Attachment 2.

- **Cost of the project was derived from prices and quantities agreed in the latest contract draft.**
- **Current annual costs for existing vendor services ($1,021,010.70) represents the average cost for the past 2 fiscal years (2019, 2020) as recorded in VISION ledger reports provided by the project team.**

- **State personnel in the above table represents the project team's best estimate of State personnel costs for *procurement* actual to date and estimated through implementation)**
- **State personnel costs for operating the *current* system represent actual FY2020 totals of $390,371.31.**
- **State personnel costs for operation the *new* system calculated as follows, reflecting State's aim to reduce staff time spent on VoIP operation by 20 hours per week, using the State-supplied estimate of $84/hr. for this level: $390,371.31 – (84 X 20 X 52 = $87,360.00) = $330,011.31.**
- **Professional Services cost represents contractual agreement with this consultant.**

5.2 COST COMPARISON:

How do the above Acquisition Costs compare with others who have purchased similar solutions (i.e., is the State paying more, less or about the same)?

VoIP providers price deployments generally on a per-user/per-month basis. The infrastructure supporting cloud-based VoIP systems is highly scalable, so providers often offer lower per-user pricing for higher user volumes. For example, a VoIP provider used by some U.S. Military Agencies (e.g., Air Force Recruiting and U.S. Army), Nextiva, offers basic VoIP service at $24.95 for 1-4 users, and the same service at **$17.95** for 100+ users.[1] An unscientific survey of VoIP per-user/per-month costs of other widely available full-service providers shows pricing generally in the **$18 to $20** range.[2] These drop somewhat as volume increases. The State of Illinois owns its VoIP system, and charges a basic internal rate of **$17.00**.[3]

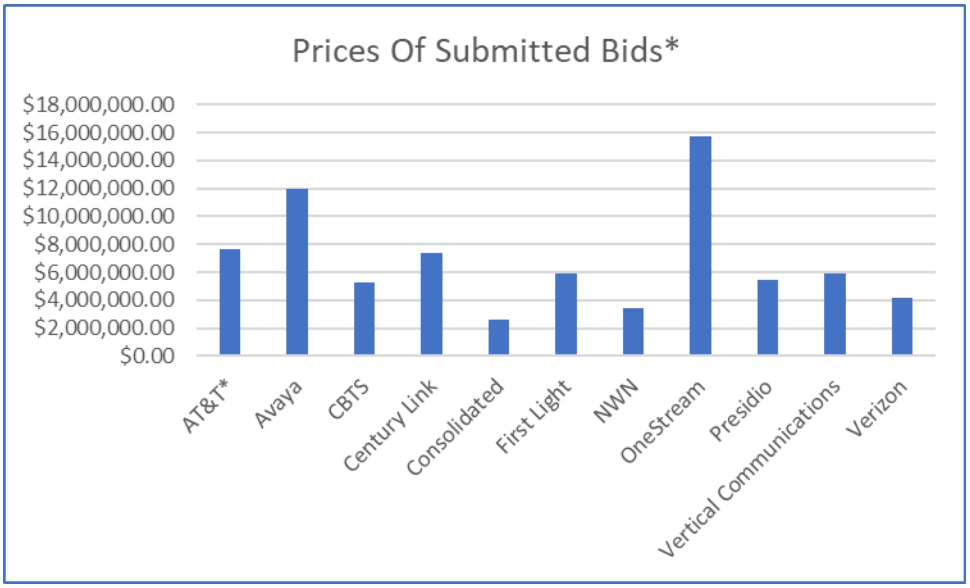
If we use the annual cost of the present project as proposed*, including the estimated cost of State personnel to operate and maintain it*, we derive a per-user/per-month cost of **$16.95** for the proposed project. This looks like a cost of "about the same" or better. Furthermore, if the State scales up the user base as expected, vendor costs to the State will increase, but State personnel costs will likely remain about the same, so that overall cost to the State will be even more favorable.

Notably, NWN's proposal was significantly less expensive than all but one of the other submitted bids, as shown in the chart below. (The one vendor proposing a lower cost declined to include implementation costs in the proposal, and so was technically unresponsive to the RFP.) *Note that this chart compares lifecycle costs as each vendor proposed; not all bids were adequately responsive to the RFP.*

[1] https://www.nextiva.com/nextiva-pricing.html

[2] https://priceithere.com/voip-phone-system-prices/

[3] https://www2.illinois.gov/sites/doit/services/catalog/telecom/Pages/voip.aspx



5.3 COST ASSESSMENT:

Are the Acquisition Costs valid and appropriate in your professional opinion? List any concerns or issues with the costs.

Yes, the costs are valid as memorialized in the current contract draft and they are appropriate in that they represent a very favorable cost to the State on a per-user/per-month basis. Extending the user base within State government is likely to result in even lower costs on that basis.

Additional Comments on Acquisition Costs:

> *At the time of review, the pricing tables in the draft contract had no quantities given for phone replacement at DPS. Determining the exact number, if any, may need to wait for a requirements determination, post-contract execution.*

6 TECHNOLOGY ARCHITECTURE REVIEW

OVERVIEW

The proposed project retains and builds upon the architecture of the State's current VoIP system, provided by the same vendor, NWN. The system is cloud-based, highly secure, employing redundancy for reliability, and built upon the same platform the State uses internally, Cisco Unified Communications (UC), an IP-based communications system integrating voice, video, data, and mobility products and applications. The vendor appears to conform to Cisco UC best practices throughout the system, which we find reassuring, as the State has knowledge and experience with Cisco UC.

The vendor operates its private cloud via two geographically diverse data centers. The data centers are highly secure, conforming to State requirements, as described in the Security Assessment below. NWN's hardware and infrastructure comprising the vendor's portion of the system are distributed between the two data centers. They mirror each other comprehensively, so that if there is a failure or network disruption affecting one data center, the other can automatically take over the UC traffic. The data centers are connected to the State's network (GOVnet) via geographically and vendor diverse Multi-Protocol Label Switching (MPLS) connections. The edge routers at the State end of these connections are located in the State's two main data centers and form the demarcation points beyond which the State manages its own network, including the VoIP endpoints. The endpoints may be hardware IP phone or video devices, or they may be software clients such as Cisco Jabber. The State has a very strong preference to manage its own network, and therefore State technical personnel configure, manage, and maintain all the GOVnet network infrastructure to support the system (rather than, for example, allowing vendor technicians to configure Cisco UC by remotely connecting to GOVnet routers). We assess this as a good practice which maintains and simplifies State network security. The system connects to the conventional (non-VoIP) landline telephone network at several points, to allow landline phones, cell phones, and VoIP phones on other publicly connected networks to call and receive calls from State VoIP phones, including long-distance calls.

The State deploys some personnel to work remotely, and of course this deployment has increased greatly during the Covid epidemic. State employees who work remotely will generally use a "soft client" for VoIP communications, rather than a hardware IP phone. This is both economical (Cisco UC includes the Jabber soft client) and productive, as desktop clients can take advantage of other forms of communication and integration with the workstation. The State currently uses several soft clients on the existing system but intends to standardize on the Cisco Jabber client. This client is available in several forms, including desktop, IOS (iPhone/iPad), and Android (smartphones and tablets). There are advantages and disadvantages to soft client deployment, although we assess that the advantages greatly outweigh the potential disadvantages.

The advantages include simplicity of deployment (no need to physically deliver hardware), elimination of capital or lease investment in hardware, integration with the desktop, and in the case of the Jabber client, ease of configuration, as the client can be configured by the State for a "one-click" configuration after download by the remote worker. (Also, see the e911 description below.) Another advantage is that

Cisco Jabber can use encryption to enable secure calling. Disadvantages include the fact that any software on a workstation is potentially a security risk (see *https://www.cisco.com/c/en/us/support/docs/csa/cisco-sa-jabber-ttcgB9R3.html* for example). We identify this as a risk **RISK_ID# _R2**. However, we reiterate that the risk is small compared to advantages, particularly if the State standardizes completely on the Jabber client.

Although the proposed project in broad terms continues the current system as described above, there are several additions and improvements in-scope:

E911 COMPLIANCE

The State's existing VoIP system is not in its entirety compliant with the new Vermont e911 rule of July 1, 2019. (It may in similar ways be non-compliant with federal law — "Kari's Law" — that went into effect in February 2020.) In particular, the State's VoIP system, called an Enterprise Communication System (ECS) in the e911 rule, must provide precise location data from a VoIP phone calling e911 even if that phone is a soft client, and must host a Location Information Server (LIS) to provide location data based on a lookup of the phone number. Other provisions require that a caller reach emergency services by dialing 911 without needing a prefix for an outside line, and that the phone reports a valid callback number.

The proposed system addresses the need for compliance by deploying and configuring a component of Cisco UC called Cisco Emergency Responder (CER). This deployment will bring the State system into compliance in conjunction with proper configuration of all State soft clients. This configuration will be accomplished in one of two ways:

- Cisco Jabber clients deployed on iPhones and Android smartphones will automatically use the cell phone's phone number for location information.
- Other soft clients will use an associated application called Sentry Gatekeeper, which is easily configured by the soft client user to provide location information. This does, however, mean that the proper configuration is subject to user error, and we identify this as a risk **RISK_ID# _R4**.

We find this plan to bring the State's system into 911 compliance to be effective and do-able. The use of the Cisco UC platform increases the likelihood of a successful integration.

DEPARTMENT OF PUBLIC SAFETY (DPS) MIGRATION

The State intends to migrate the DPS non-PSAP (Public Safety Answering Point) phone system to the State VoIP system via this project. As part of this migration, the vendor and the State will deploy the DPS phones at "survivable sites" via Cisco Unified Survivable Remote Site Telephony (SRST). This is a technology that equips the edge routers at DPS sites in such a way that if the VoIP system fails for any reason, the site can continue to make and receive calls via the conventional landline telephone network (also known as the Public Switched Telephone Network, or PSTN).

We think the deployment of Cisco SRST is a reasonable, reliable, and well-tested choice. Like the other communication components of the system, it shares a common platform with the rest of the State system.

NWN EXPERIENCE MANAGEMENT PORTAL (EMP)

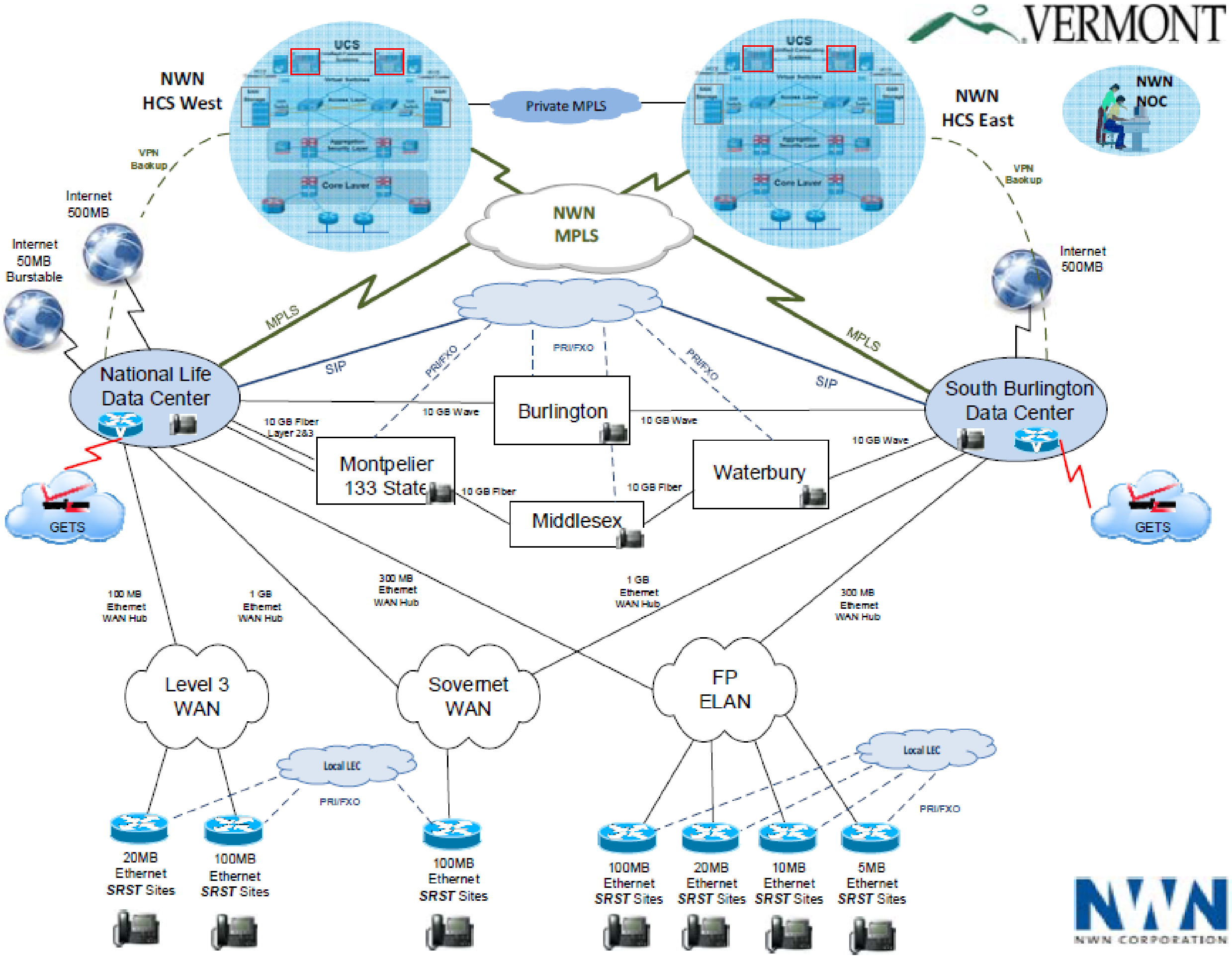
As part of this project, the vendor will migrate the State's current VoIP management platform to NWN's newer EMP system. EMP modernizes some management capabilities the State currently has and adds enhanced reporting and analysis capabilities. It improves access to vendor support services and is said to enhance the "self-service" capabilities, so that State technicians and engineers can do most internal VoIP tasks without vendor support services. The State especially intends to manage its own Move-Add-Change-Delete (MACD) processes for moving and renumbering phones.

BILLING DIRECT TO AGENCIES/DEPARTMENTS

Although not purely and architectural aspect, the new project moves billing into the hands of the vendor, who will provide billing services to State Agencies or other units. (Payments still remain internal to the State.) This is a significant change that frees some time (the project team estimates 20 hours/week) currently engaging State personnel for billing, with the freed time to be used for other tasks appropriate to their skills. This seems like a good decision, as the vendor probably has the data to automate this process more easily.

NETWORK DIAGRAM

The diagram below, provided by the vendor, is a good representation of the logical configuration of the State’s VoIP network:



After performing an independent technology architecture review of the proposed solution, please respond to the following.

6.1 STATE'S ENTERPRISE ARCHITECTURE GUIDING PRINCIPLES

6.1.1 A. ASSESS HOW WELL THE TECHNOLOGY SOLUTION ALIGNS WITH THE BUSINESS DIRECTION

This project addresses an aspect of Executive Order No. 06-17 (creating the ADS) which mandates "Utilization of technology skills and resources across departments for the benefit of all agencies and departments;" The ADS Shared Services portfolio addresses government-wide IT services. The present project aligns exactly with that mandate.

6.1.2 B. ASSESS HOW WELL THE TECHNOLOGY SOLUTION MAXIMIZES BENEFITS FOR THE STATE

The project realizes cost savings for the State while providing improved service. The e911 capability removes a potential liability while increasing safety for State employees. The architecture employed by the system can be easily scaled up to more end users when the State needs to do so and provides a platform for potential future modernization via Contact Center replacement.

6.1.3 C. ASSESS HOW WELL THE INFORMATION ARCHITECTURE OF THE TECHNOLOGY SOLUTION ADHERES TO THE PRINCIPLE OF INFORMATION IS AN ASSET

Even though the solution is not intrinsically data-centric, the architecture is highly secure and resilient specifically *because* the State recognizes the value of information that will traverse the system (i.e., intra-governmental conversations) and required a solution that would meet that need. The State's experience with the underlying Cisco UC platform boosts confidence that those requirements are met.

6.1.4 D. ASSESS IF THE TECHNOLOGY SOLUTION WILL OPTIMIZE PROCESS

Aside from the obvious benefits of a reliable and well-functioning phone system, the transfer of billing functions from State to vendor will improve Agency/Departmental fiscal process (because the existing system does not provide those units with adequate and timely information). It will also free State personnel time that is best used for other tasks.

6.1.5 E. ASSESS HOW WELL THE TECHNOLOGY SOLUTION SUPPORTS RESILIENCE-DRIVEN SECURITY.

Please see the Security Assessment, below. The solution closely adheres to security best practices at all levels of implementation, from secure and redundant hosting and communications links to desktop client encryption, ensuring reasonably reliable communications even in the event of unforeseen failures, with even more extensive reliability in the survivable sites. Cisco UC is a mature platform, widely used by government and industry, with a very deep history of security features and flexible configurability.

6.2 SUSTAINABILITY

Financially, the project is sustainable because it is scalable in such a way that per-user costs are likely to decrease if the State expands deployment.

Technologically, it is sustainable because it employs a platform (Cisco UC) which is so widely used that it is likely to be supported for many years.

Environmentally, it supports sustainability because it posits the increased use of software clients and a decreased use of hardware IP phones, decreasing the manufacturing carbon footprint and use of rare earths. That said, it is true that large data centers are very energy intensive, so there is some question about the environmental impact of cloud-based solutions.

6.3 HOW DOES THE SOLUTION COMPLY WITH THE ADS STRATEGIC GOALS ENUMERATED IN THE ADS STRATEGIC PLAN OF JANUARY 2020?

6.3.1 A. Leverage successes of others, learning best practices from outside Vermont.

The Cisco UC platform is a mature and very widely used product. It has an extensive support base from Cisco and a worldwide user base, eager to share experience and advice. The State adopted this platform several years ago and continues to draw on all these resources to build knowledge and good practice.

6.3.2 B. Leverage shared services and cloud-based it, taking advantage of IT economies of scale.

The present project targets exactly these points. For an analysis of scalable costs, see Cost Assessment, above. It is also notable that, as the State has expanded its VoIP needs, the cost to the vendor has decreased, supporting the notion that shared services can be economically scalable.

6.3.3 C. Adapt the Vermont workforce to the evolving needs of State government.

The Covid epidemic and the potentially permanent changes in remote working have demonstrated how useful a technologically flexible State network can be. The increased use of VoIP soft clients in the present project enables these changes while maintaining the level of security and confidentiality that was expected in the closer office environment. It remains to be seen how government and the workforce adopt and adapt to these changes, but the VoIP system seems to us to be flexible enough to accommodate various scenarios.

6.3.4 D. Apply enterprise architecture principles to drive digital transformation based on business needs.

An architecture assessment was performed in several stages on the best proposal candidates in the procurement process. Scoring on functional and non-functional requirements played a significant role in the initial and final choices of vendors. Enterprise Architecture needs have continued to inform the contract negotiations and improve the agreement as it approaches finalization.

6.3.5 E. Couple IT with business process optimization, to improve overall productivity and customer service.

The present project includes improved reporting, system use analysis (call detail, SIP traffic), and custom reports as needed. These all support a more efficient and productive use of ADS time in managing the VoIP system. Importantly, the move of billing from State to vendor is likely to result in smoother fiscal processes in billed units.

6.3.6 F. Optimize IT investments via sound project management.

Project management requirements are very forward and prominent in the State's RFP. Vendors were required to meet very specific State requirements and to respond in detail about their own project management policies, processes, and personnel. The selected vendor responded with more than adequate detail and supporting evidence (resumes, etc.).

On the State side, project management and oversight has been comprehensive and competent from the start.

The State is clearly strongly and most importantly, *clearly*, supporting sound project management through specificity of requirements and through project team process.

6.3.7 G. Manage data commensurate with risk.

Generally, N/A. Data in the form of intra-governmental conversation does of course traverse the system, and the security and privacy features are very good, as described in the Security Assessment below.

6.3.8 H. Incorporate metrics to measure outcomes.

In the IT-ABC form, the project team identified three business justifications. The first is a compliance value and refers to compliance with the e911 rule. This result will be measure by testing performed by the e911 Board. The second is improved customer service for support tickets and MACD orders, measured by a reduction in time needed to achieve or resolve the requests. It seems likely that the improved MACD capabilities and the EMP support platform will achieve this goal. The third is improved reporting to be used for bill back to State Agencies. In fact, this need will be addressed by the vendor handling billing direct to State units.

6.4 COMPLIANCE WITH THE SECTION 508 AMENDMENT TO THE REHABILITATION ACT OF 1973, AS AMENDED IN 1998

The end-user experience of the proposed solution is almost entirely based on Cisco technology. Cisco states this on their website:

Cisco complies with accessibility laws and strives to supply end-user devices that conform and support the U.S. Access Board's standards as referenced in Section 508 of the Rehabilitation Act.

They also publish their Accessibility policy in which they state that they "*Evaluate accessibility and usability throughout the product design, development, and fabrication processes as early and consistently as possible.*"[4]

Since the design and implementation of the proposed solution is entirely the responsibility of the vendor, we think that Cisco's statements and policy address this question.

6.5 DISASTER RECOVERY

The vendor employs Cisco recommended best practices for disaster recovery, coupled with governmental standards for hosting. These include Failover Redundancy (e.g., multiple servers that back each other up), Redundant links (such as the MPLS connections to SOV, provided by diverse service providers), and Geographical Diversity. The vendor's Data Centers are Tier 3 rated or higher, with disaster recovery procedures tested as required for accreditation including SSAE-18 SOC1 Type 2 and SSAE-16 SOC2. These accreditations are consistent with the State's requirements for secure cloud hosting. The Cisco UC applications are deployed by the vendor with application-level redundancy to protect against any complete failure of a UC application.

The geographically diverse data centers are run in an active/active mode. This means that both centers are in hot standby mode for each other. This increases the load capability, as both centers are sharing the load, but it also means that any failure of one data center is in theory immediately covered by the other.

Disaster recovery in a real-time communication system is different from recovery in, for example, a database system. Real-time systems prioritize availability and redundancy, as there is less need for recovering lost data. We see this vendor as pursuing best practices for very high availability, and State experience with their system has been very favorable thus far.

[4] https://www.cisco.com/c/en/us/about/accessibility.html#~accessibility-policy

6.6 DATA RETENTION

In this system, data retention primarily refers to data owned by the vendor and related to vendor operations, such as system logs, vendor database logs, etc., and not to State-owned data (aside from call detail and billing data). In the draft contract, the vendor has shared their current security policy, including data retention policies. In that respect, they are interesting in that they show the vendor's foresight, reliability, and diligence, but not particularly applicable to State needs.

6.7 SERVICE LEVEL AGREEMENT

6.7.1 WHAT ARE THE POST IMPLEMENTATION SERVICES AND SERVICE LEVELS REQUIRED BY THE STATE?

The State did not require specific post implementation services nor state specific required service levels in the RFP, but instead required bidders to attach their "standard" service level agreement (SLA) and to answer a number of questions covering:

- Customer Phone &/or Email Support
- Incident/Security Breach Notification and Process
- Data Management
- Hosting
- Scheduled Maintenance/Downtime
- System Upgrades
- Bug Fixes and Minor Enhancements
- Disaster Recovery
- Reporting

The proposed vendor's responses to these questions were evaluated and scored by the project leaders, enterprise architect, and security analyst as needed, and were found to be generally acceptable. Further questions to clarify any responses were asked by the State and answered to the project team's satisfaction.

We also reviewed the vendor's responses in these areas, and found them to be quite comprehensive, reasonable, and following industry best practices.

6.7.2 IS THE VENDOR PROPOSED SERVICE LEVEL AGREEMENT ADEQUATE TO MEET THOSE NEEDS IN YOUR JUDGMENT?

Yes. The latest draft contract contains detailed Service Level Agreement (SLA) targets for both system performance, with a primary System Availability target of 99.99%, similar availability for production, support, disaster recovery, and any other environments. In the event targets are not met, there is a 3-tiered Service Level credit for the month in which the default occurred. There are additionally targets for other support and escalation processes provided.

We find this SLA to be unusually comprehensive and specific, and judge that it will serve the State well and encourage the vendor to best performance.

6.8 SYSTEM INTEGRATION

6.8.1 IS THE DATA EXPORT REPORTING CAPABILITY OF THE PROPOSED SOLUTION CONSUMABLE BY THE STATE?

The EMP program produces reports and visual representations of:

- Call reporting and Analytics
- SIP reporting and Analytics (use of telecom intra-State communications leased by the State)
- Provisioning and Administration Portals (such as MACD)
- Billing Detail Reporting

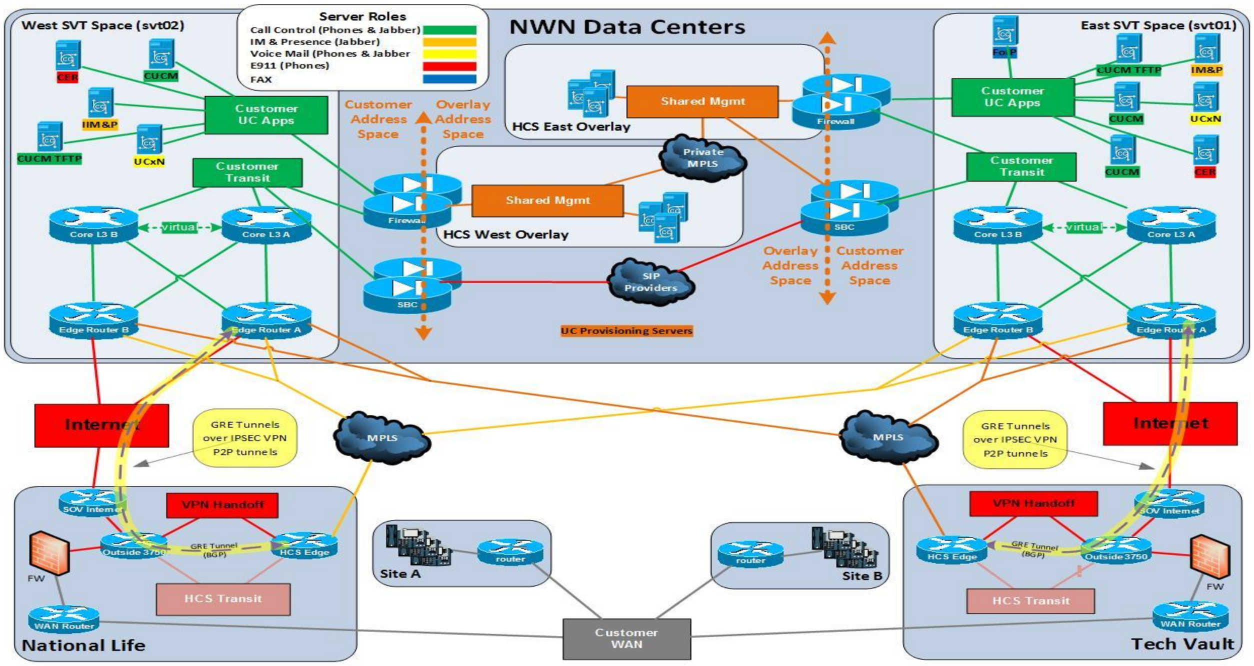
All of these are potentially consumable by the State. Additionally, the State sometimes requests custom reports from the vendor, and a number of these are reserved for the State in the contract at no additional cost.

6.8.2 WHAT DATA IS EXCHANGED AND WHAT SYSTEMS (STATE AND NON-STATE) WILL THE SOLUTION INTEGRATE/INTERFACE WITH?

The VoIP system does not directly integrate with any State data systems. The EMP program produces reports, and these may possibly be manually moved into spreadsheets or other database programs.

Additional Comments on Architecture:

Networking entity diagram (provided by vendor):


West SVT Space (svt02)
Server Roles
Call Control (Phones & Jabber) 🟩
IM & Presence (Jabber) 🟧
Voice Mail (Phones & Jabber 🟨
E911 (Phones) 🟥
FAX 🟦
NWN Data Centers
East SVT Space (svt01)
CER
CUCM
IIM&P
CUCM TFTP
UCxN
Customer UC Apps
Customer Transit
Core L3 B
virtual
Core L3 A
Edge Router B
Edge Router A
Customer Address Space
Overlay Address Space
Shared Mgmt
HCS East Overlay
Firewall
Private MPLS
Shared Mgmt
HCS West Overlay
SBC
SIP Providers
Overlay Address Space
Customer Address Space
UC Provisioning Servers
FoIP
CUCM TFTP
IM&P
Customer UC Apps
CUCM
UCxN
CUCM
CER
Customer Transit
Core L3 B
virtual
Core L3 A
Edge Router B
Edge Router A
Internet
GRE Tunnels over IPSEC VPN P2P tunnels
MPLS
MPLS
GRE Tunnels over IPSEC VPN P2P tunnels
Internet
SOV Internet
VPN Handoff
Outside 3750
GRE Tunnel (BGP)
HCS Edge
FW
HCS Transit
WAN Router
National Life
Site A
router
router
Site B
Customer WAN
VPN Handoff
SOV Internet
HCS Edge
GRE Tunnel (BGP)
Outside 3750
FW
HCS Transit
WAN Router
Tech Vault

7 ASSESSMENT OF IMPLEMENTATION PLAN

The proposed project in large part continues operation of the existing SOV VoIP system, provided by the same vendor. As such, there is no implementation plan for the system as a whole – the system is already in place. Implementation of enhancements to the system consist of the following:

- E911 compliance
  The existing system already supports some e911 functions. The vendor with the State will implement Cisco Emergency Responder to provide functions needed for full compliance, in particular dispatchable location information on 911 calls and implementation of a Location Information Server (LIS).
- Migration of Public Safety users and survivable site (SRST) implementation
- Transition to vendor's EMP reporting portal solution (primarily training/support on the State side)
- Billing processes (primarily consultation for transition on the State side)

The comments below refer to the vendor's implementation plan for e911 compliance.

After assessing the Implementation Plan, please comment on each of the following.

7.1 THE REALITY OF THE IMPLEMENTATION TIMETABLE

Table 7 (Project Milestones), above, lists the phases of e911 enhancement implementation. In the event some phases may overlap, but if taken sequentially, the total implementation from Initiation to Deployment would be 110 days. Since this implementation primarily addresses dispatchable location information and an LIS and other 911 functions are already operational, we see no reason to find this timetable unrealistic for such a project. We note that the State will also have responsibilities that may impact the timetable (see 7.3.7, Implementation, below), but the State assesses that these responsibilities are well within its capabilities with current staff.

7.2 READINESS OF IMPACTED DIVISIONS/ DEPARTMENTS TO PARTICIPATE IN THIS SOLUTION/PROJECT

(Consider current culture, staff buy-in, organizational changes needed, and leadership readiness).

The project team is enthusiastic and ready for contract execution after a fairly long and sometimes arduous procurement process. The proposed project resolves some previous issues or frustrations (using State resources for billing, some confusion about custom reports from the vendor) and will likely lead to satisfaction among staff. We encountered no resistance on the project team to the choice of vendor. Relevant staff have informed us that past experience with this vendor has been very good.

We have been told by the project team leaders that knowledge about the State VoIP network is somewhat concentrated among a small number of long-term State personnel. Should those individuals become unavailable due to illness, retirements, or any other reason, implementation of a new system could be delayed. While we have no imminent reason to expect this to be a problem, we do identify it as a risk **RISK_ID# _R3** and recommended that the State mitigate this risk by cross training employees or similar approaches. The State agreed and responded that the business lead is already taking steps to do this from a contract management perspective and the network team also cross trains staff as best practices.

7.3 DO THE MILESTONES AND DELIVERABLES PROPOSED BY THE VENDOR PROVIDE ENOUGH DETAIL TO HOLD THEM ACCOUNTABLE FOR MEETING THE BUSINESS NEEDS IN THESE AREAS:

7.3.1 A. PROJECT MANAGEMENT

Project Management milestones, as listed in the draft contract, include:

- Initiate Project Kick Off meetings to review the scope with the project team and develop the project management plan.
- Assess the current target infrastructure.
- Design, validate, test and pilot the new environment.
- Prepare Proof of Concept and build the initial unit.
- Execute phased deployment, integrations, and cut over.
- Transition to the new platform

Project Management deliverables, as listed in the draft contract, include:

- Project Plan
- Project Schedule
- Communications Plan
- Scope Document
- Project Change Request Template
- Meeting Minutes
- Risk Matrix

Both milestones and deliverables are consistent with State requirements and Project Management Book of Knowledge (PMP) processes, and map cleanly to the implementation phases in the above table. The vendors project management team is well-credentialed and experienced. We have no concerns with project management.

7.3.2 B. TRAINING

The vendor will provide “train the trainer” support as part of the e911 implementation. This is consistent with State expectations, and past experience with the vendor has been good. We note also that the EMP platform includes access to on-line training and knowledge base resources, which will support the VoIP system as a whole.

7.3.3 C. TESTING

Testing will be consistent with Cisco best practices. After implementation, the State will test the e911 functions via the e911 Board.

7.3.4 D. DESIGN

Design is consistent with Cisco best practices. We have no concerns with the vendor's competence.

7.3.5 E. CONVERSION (IF APPLICABLE)

N/A

7.3.6 F. IMPLEMENTATION PLANNING

The vendor's proposal describes in some detail their general implementation approach. This approach is consistent with PMBOK practices and emphasizes "up-front discovery and design." The outline used for implementations is as follows:

1. Initiate Phase:
    a. External Kickoff PPT slides
    b. Initiate Phase Signoff
2. Assess/Design Phase:
    a. UC Design Document & Signoff
    b. UCCE Design Document & Signoff
    c. Assess/Design Phase Signoff
3. Prepare Phase:
    a. Infrastructure Complete (UC & UCCE)
    b. Applications Complete (UC & UCCE)
    c. Configuration (UC & UCCE)
    d. System Testing (UC & UCCE)
    e. Pilot Group (UC & UCCE)
    f. End User Training & Documentation (UC & UCCE)
    g. Administrator Training & Documentation (UC & UCCE)
    h. User Acceptance Testing Signoff (UC & UCCE)
    i. Prepare Phase Signoff
4. Execute Phase:
    a. Site Turn-up & Testing Signoff per site/cutover
    b. Execute Phase Signoff (based on contract)
    c. Transition Phase:
    i. Transition Phase Signoff

Clearly this outline refers to implementations of whole VoIP systems (i.e., Cisco UC), but we find it to be a good shorthand for the vendor's general approach to implementation. We find it to be consistent with the State's expectations and business needs.

7.3.7 G. IMPLEMENTATION

The implementation of the e911 enhancements will require tasks to be performed by both State and vendor. State responsibilities include:

- Network Switches
  - Provide list of models, IOS versions and quantities for each location, including IP addresses and SNMP read-only string.
  - Switches must be Cisco models supported by CER running a supported IOS version.
  - Create SNMP Read Only string for Emergency Responder on each switch.
  - Verify that CDP (Cisco Discovery Protocol) is enabled on each switch.
  - Verify all switch port connections and locations are properly identified.
  - Verify all switch ports have correct descriptions to map to proper ERL (Switch port descriptions are alpha numeric strings up to 240 characters)
  - Verify the physical location of all phones.
  - Provide building signage for phone locations.
  - Direct inward dialing numbers (DIDs)
  - Order (1) DID per station from NWN for Emergency Responder ELINs
  - Create test plan & perform validation.

The vendor's deliverables, in addition to Project Management deliverables described above, include:

- Emergency Responder
  - Add switches.
  - Add the location of the switch port.
  - Add DIDs for Emergency Responder ELINs
  - Add ERLs.
  - Add ELINs.
  - Configure Notifications to State distribution lists as specified.
- Communications Manager
  - Add unique DIDs (1 per phone)
  - Add DIDs to the SIP Session Border Controllers (SBCs)
  - Add ERL translation patterns.
- Bandwidth.com
  - Add DIDs.
  - Update ALI database

These deliverables demonstrate that the vendor has demonstrated adequate forethought to this implementation, and that it is consistent with Cisco requirements. The clear delineation of State and vendor responsibilities should help advance the implementation timetable and meet the business needs of the State.

7.4 DOES THE STATE HAVE A RESOURCE LINED UP TO BE THE PROJECT MANAGER ON THE PROJECT? IF SO, DOES THIS PERSON POSSESS THE SKILLS AND EXPERIENCE TO BE SUCCESSFUL IN THIS ROLE IN YOUR JUDGMENT?

Yes. We have worked with this project manager in previous engagements, and find her to be highly competent, meticulous, knowledgeable about PM best practices, and good at managing the project teams process and timetable. Her skills are very appropriate to this project.

Additional Comments on Implementation Plan:

Conditions resulting from the ongoing Covid-19 pandemic could lead to restrictions on movement, social interaction, in-person working, or other aspects of implementation, interfering with work by State and/or vendor employees assigned to the project. We identify this as a risk **RISK_ID# _R1** although at the time of writing the danger seems lessened. The State responds as follows:

The State accepts the risks. The State believes staying with the current vendor reduces risks due as few implementation changes will be needed and all installation can be performed remotely.

We concur with this response.

8 COST ANALYSIS AND MODEL FOR BENEFIT ANALYSIS

8.1 ANALYSIS DESCRIPTION:

Provide a narrative summary of the cost benefit analysis conducted.

Tangible cost/benefit analysis is presented on Attachment #2, Cost Spreadsheet. Vendor costs, State personnel costs, and any other costs are derived as described in Section 5.1 Cost Validation, above. Compared to these costs on a lifecycle basis are projections of the current costs of the existing system for a comparable period. This results in a positive or negative net tangible benefit for the lifecycle of the project.

Intangible benefits are derived from discussions with the project team, review of project documentation, and analysis of the project as a whole.

8.2 ASSUMPTIONS:

List any assumptions made in your analysis.

- For comparison purposes, current costs are projected to stay the same for the lifecycle of the project.
- The project team's projection of a reduction of 20 hours per week for operation and maintenance of the system due to transition of billing to the vendor is assumed to be valid.

8.3 FUNDING:

Provide the funding source(s). If multiple sources, indicate the percentage of each source for both Acquisition Costs and on-going Operational costs over the duration of the system/service lifecycle.

The system is 100% state funded. Agencies and Departments or other units are billed for usage. Currently this billing is done internally, but the present project proposes to move the billing (but not collection) function to the VoIP vendor.

8.4 TANGIBLE COSTS & BENEFITS:

Provide a list and description of the tangible costs and benefits of this project. Its "tangible" if it has a direct impact on implementation or operating costs (an increase = a tangible cost and a decrease = a *tangible benefit). The cost of software licenses is an example of a tangible cost. Projected annual operating cost savings is an example of a tangible benefit*.

Over the lifecycle of the project, the State would realize a benefit of

$ 1,383,657.21

to acquire and operate the proposed project,
compared to continuing the operation of the existing system.

This tangible benefit is due to a reduction in charges by the vendor compared to their previous charges, and a slight reduction in State personnel costs *for the project*.

8.5 INTANGIBLE COSTS & BENEFITS:

Provide a list and descriptions of the intangible costs and benefits. Its "intangible" if it has a positive or negative impact but is not cost related. Examples: Customer Service is expected to improve (intangible benefit) or Employee Morale is expected to decline (intangible cost.

- **Full e911 rule and federal law compliance for the VoIP system, increasing employee and public safety, decreasing State liability, and enhancing State reputation.**
- **Customer Service Improvement**
  - **Improved reporting capabilities – more flexibility to run reports needed for billing.**
  - **Long Distance call detail**
  - **Call detail – when requested – ideally users could query this on a self-service portal.**
  - **Billing Code information accuracy**
  - **Improved customer service – improved accuracy of moves/adds/changes/deletes.**
- **Standardization of remote soft phone client, increasing reliability and security and decreasing support requirements, to increase flexibility for remote working.**

8.6 COSTS VS. BENEFITS:

Do the benefits of this project (consider both tangible and intangible) outweigh the costs in your opinion? Please elaborate on your response.

This project is clearly beneficial to the State, in financial terms of course, but importantly in bringing the State into e911 rule compliance, which is absolutely necessary. E911 compliance might conceivably have been accomplished via a standalone project, but when the State explored

that in 2019, it concluded that the approaches proposed were incomplete and unsatisfactory. The present project achieves compliance along with significant cost savings and service enhancement.

8.7 IT ABC FORM REVIEW:

Review the IT ABC form (Business Case/Cost Analysis) created by the Business for this project. Is the information consistent with your independent review and analysis? If not, please describe. Is the lifecycle that was used appropriate for the technology being proposed? If not, please explain.

The IT ABC form projected a 5-year lifecycle total at current costs as $7,431,360.00. This is reasonably close to our projected figure of $7,826,410.05.

The IT ABC form proposed total lifecycle cost was $2,722,016.00, compared to our calculation of $6,442,752.84, 237% higher. Partly, this is due to the addition of Public Safety and survivable site costs in the proposed project.

The IT ABC form therefore project a savings to the State of $4,709,344.00, while we project a savings of $1,383,657.21.

The other benefits projected on the IT ABC form (e911 compliance, improved reporting, better billing) are entirely consistent with the benefits we anticipate from the proposed project.

Additional Comments on the Cost Benefit Analysis:

none

9 ANALYSIS OF ALTERNATIVES

The State initially selected a different vendor (CBTS) and undertook contract negotiations. Over a period of weeks, the State concluded that this vendor was unable or unwilling to meet State requirements comprehensively. After some discussion, the State decided to select its second choice (NWN), that also scored highly overall. The State finds NWN to be very responsive to State requirements, capable of meeting them comprehensively, and additionally has had a very good experience with the vendor since 2015.

9.1 PROVIDE A BRIEF ANALYSIS OF ALTERNATE TECHNICAL SOLUTIONS THAT WERE DEEMED FINANCIALLY UNFEASIBLE.

The State pursued a VoIP solution to its voice intra- and extra-governmental communication needs beginning in 2015, when it first employed NWN to provide VoIP service. This replaced a system of conventional telephony based on 50-year-old technology, employing multiple Centrex contracts and increasingly complex multi-line phones and fax machines, operating alongside but separated from email, video, and other communication networks. The existing telephone system was increasingly expensive and inflexible in the face of frequent need to move phones and reconfigure office space, introducing additional personnel cost to maintain the system.

At least two of the bids submitted by potential vendors (see 5.2 Cost Comparison, above) proposed pricing that the procurement team assessed as unfeasible. These proposals were 3 to 4 times as expensive as the selected vendor with no significant additional benefits, at $11,964,912.80 (Avaya) and $15,768,107.25 (OneStream). We note that neither of these proposals scored as high overall in combined categories (including but not exclusive to pricing) as the 3 first-round finalists.

9.2 PROVIDE A BRIEF ANALYSIS OF ALTERNATE TECHNICAL SOLUTIONS THAT WERE DEEMED UNSUSTAINABLE.

Some large enterprises (e.g., the State of Illinois) choose to develop and host VoIP solutions internally. This approach may be viable when there is a broad and deep personnel resource including development and testing facilities and an extensive and appropriately redundant data center environment. The State does not have these capabilities and has chosen to pursue an explicit strategic choice to embrace cloud-based IT solutions to promote flexibility and sustainability. We think the State’s approach is exactly right. We would point out as well that the State of Illinois seems to have a per-user/per-month cost that is no lower than that of Vermont’s under the proposed project.

9.3 PROVIDE A BRIEF ANALYSIS OF ALTERNATE TECHNICAL SOLUTIONS WHERE THE COSTS FOR OPERATIONS AND MAINTENANCE WERE UNFEASIBLE.

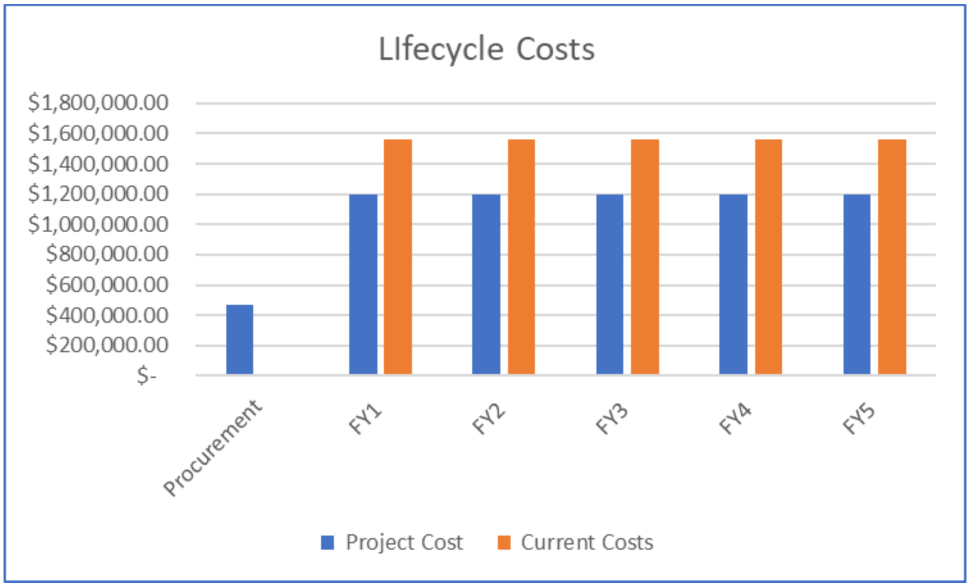
Because the required solution is cloud-based, operations and maintenance costs comprise the greater part of the lifecycle cost, especially if the costs are not hardware-intensive (as might be the case if the State were procuring a large number of hardware IP phones). Therefore, the total costs described in 9.1 above apply identically here.

10 IMPACT ANALYSIS ON NET OPERATING COSTS

10.1 INSERT A TABLE TO ILLUSTRATE THE NET OPERATING COST IMPACT.

Table 9 - Net Operating Cost Impact

	Procurement	FY1	FY2	FY3	FY4	FY5	Total
Project Cost	**$471,763.89**	**$1,194,197.79**	**$1,194,197.79**	**$1,194,197.79**	**$1,194,197.79**	**$1,194,197.79**	**$6,442,752.84**
Current Costs	**$ 0**	**$1,565,282.01**	**$1,565,282.01**	**$1,565,282.01**	**$1,565,282.01**	**$1,565,282.01**	**$7,826,410.05**
Total Cost	**$471,763.89**	**$(371,084.22)**	**$ (371,084.22)**	**$ (371,084.22)**	**$(371,084.22)**	**$(371,084.22)**	**$(1,383,657.21)**



10.2 PROVIDE A NARRATIVE SUMMARY OF THE ANALYSIS CONDUCTED AND INCLUDE A LIST OF ANY ASSUMPTIONS.

The table and chart represent the totals for annual and lifecycle costs for the proposed project and hypothetical lifecycle at current costs.

For each of the component costs that make up these totals, see Attachment #2, Cost Spreadsheet. For the sources we used to derive those component costs, see Section 5.1 Cost Validation, above.

Assumptions include:

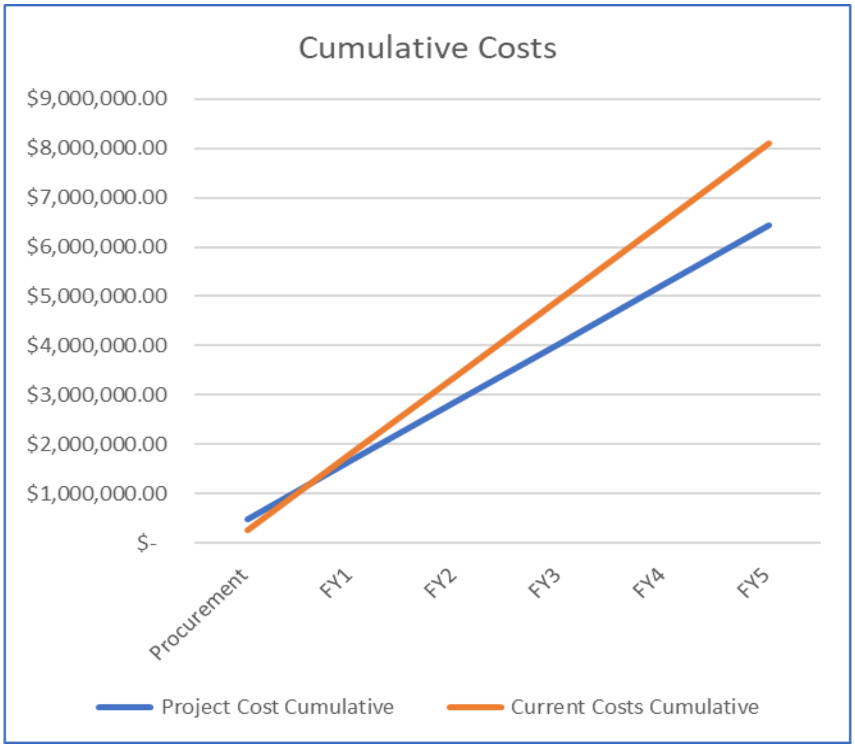
- For comparison purposes, current costs are projected to stay the same for the lifecycle of the project.
- The project team's projection of a reduction of 20 hours per week for operation and maintenance of the system due to transition of billing to the vendor is assumed to be valid.

10.3 EXPLAIN ANY NET OPERATING INCREASES THAT WILL BE COVERED BY FEDERAL FUNDING. WILL THIS FUNDING COVER THE ENTIRE LIFECYCLE? IF NOT, PLEASE PROVIDE THE BREAKOUTS BY YEAR.

No federal funding is anticipated for this project.

10.4 WHAT IS THE BREAK-EVEN POINT FOR THIS IT ACTIVITY (CONSIDERING IMPLEMENTATION AND ON-GOING OPERATING COSTS)?

	Procurement	FY1	FY2	FY3	FY4	FY5
Project Cost Cumulative	$471,763.89	$1,665,961.68	$2,860,159.47	$4,054,357.26	$5,248,555.05	$6,442,752.84
Current Costs Cumulative	$0.00	$1,565,282.01	$3,130,564.02	$4,695,846.03	$6,261,128.04	$7,826,410.05
Cumulative Cost Savings	-$471,763.89	-$100,679.67	$270,404.55	$641,488.77	$1,012,572.99	**$1,383,657.21**



The chart above shows the cumulative cost of the proposed project (blue line) compared to current costs extended over the lifecycle (orange line). After initial procurement costs (which of course are zero for the current system), the lower annual operating costs quickly establish a break-even point within the first year of operation.

11 SECURITY ASSESSMENT

Assess Information Security alignment with State expectations. ADS-Security Division will support reviewer and provide guidance on assessment.

11.1 WILL THE NEW SYSTEM HAVE ITS OWN INFORMATION SECURITY CONTROLS, RELY ON THE STATE'S CONTROLS, OR INCORPORATE BOTH?

The system will incorporate both. The State portion of the system resides on the State's GOVnet network, and to the extent that it incorporates soft clients, on the computer systems and other devices used by remote workers. The State is responsible for security controls on the supporting infrastructure: routers, workstations, etc.

The vendor is responsible for information security controls on the rest of its cloud-based system, both in terms of data center security, application security, and data movement security.

11.2 WHAT METHOD DOES THE SYSTEM USE FOR DATA CLASSIFICATION?

There is potential for some confusion, because the vendor must look at data classification in two different ways.

One is data classification for data internal to the vendor, which the vendor protects because disclosure could cause a risk to NWN or its affiliates. The vendor provides this internal policy, which identifies 3 data classification risk levels (highly confidential, reasonably confidently, and public). This classification is of little use to the State, except insofar as damage to the vendor's corporate well-being might impact service quality to the State.

Second is data classification of State-owned data which may be present on the system. These classifications are listed in tabular form in the RFP bidder response form and in the draft contract, and comprise the following:

- Publicly available information
- Confidential - Personally Identifiable Information (PII)
- Payment Card Information
- Federal Tax Information
- Personal Health Information (PHI)
- Affordable Care Act Personally Identifiable Information (PII)
- Medicaid Information
- Prescription Information
- Student Education Data
- Personal Information from Motor Vehicle Records
- Criminal Records
- Other: (FISMA, federal VoIP 911, Communications Act 2010)

The bidder response form requires the bidder to describe how they comply with each of the State and Federal standards the form lists for the categories above. In the vendor's original proposal, the vendor indicated that several of these categories were not applicable (N/A). The State disagreed, since all these types of data are potentially transmitted through the system, in various forms (conversations, video, fax over IP, etc.), and required the vendor to respond in full in the context of contract negotiations.

The vendor responded to this requirement by pointing to several aspects of their security certification audits (such as SOC2) and to several vendor security policies included as attachments to the draft contract. Although the audits and policies do indeed address the data compliance requirements, we noted that these attachments carried disclaimers from the vendor that the attached policies are "for reference only and is at the sole discretion of NWN to modify. NWN will not be held to these policies via the contract with the State of Vermont." We initially identified this situation as a risk to the project; however, the State's response indicates that the State's Attorney General's Office "has recommended that these polices are not in the contract because the vendor can update policies at their will but must give sufficient notice to the State when those policies are being updated." We defer to the AGO's experience and judgment and remove this concern.

In this light, we find that the vendor's data classification system is comprehensive and adequate.

11.3 WHAT IS THE VENDOR'S BREACH NOTIFICATION AND INCIDENT RESPONSE PROCESS?

The vendor complies fully with the State's Breach Notification law. Attachment H of the draft contract describes the vendor's Customer Facing Security Policy, which includes the relevant description of their internal notification and incident response process. The vendor responds to a list that includes, but is not limited to:

- Unusual or apparently malicious use of information assets;
- Malicious code (viruses, worms, or malicious software);
- Unauthorized information access, usage, and disclosure;
- Unauthorized physical access and usage;
- Any incident whereby a user, either directly or by using a program, performs functions for which such user does not have authorization;
- Any actions involving NWN's applications, information systems, information, or electronic devices in violation of company policy or applicable laws or regulations.

These or other potential security incidents are reported to an internal Computer Security Incident Response Team, which investigates, and if necessary takes reasonable and necessary steps to correct and mitigate any damage. In the event of a reportable security breach involving State of Vermont Sensitive Information, NWN will notify the State of such security breach without unreasonable delay. To the extent possible, NWN will provide the State with the information required to be provided by the customer in its notification to affected individuals, as applicable.

To support the incident response plan, the vendor conducts annual tests of the plan via tabletop exercises, simulations, or other comprehensive exercises.

The State Security Analyst assigned to this project concludes that this policy is adequate and appropriate, and we concur.

11.4 DOES THE VENDOR HAVE A RISK MANAGEMENT PROGRAM THAT SPECIFICALLY ADDRESSES INFORMATION SECURITY RISKS?

Yes, the vendor describes their internal risk management policy for security risks in sufficient detail. In brief, the vendor has an internal Security Committee that identifies foreseeable internal and external risks, and responds with an internal report covering:

- NWN's compliance with the Information Security Program
- Risk Assessment and Annual Loss Expectancy
- Independent testing results
- Security Incidents or violations and management's response
- Recommendations for changes to NWN's Information Security Program

And recommends action to mitigate or otherwise respond to the risks. The policy is appropriate and adequate.

11.5 WHAT ENCRYPTION CONTROLS/TECHNOLOGIES DOES THE SYSTEM USE TO PROTECT DATA AT REST AND IN TRANSIT?

Per the project’s Security Analyst, the vendor employs encryption technologies for data in transit and at rest that meet the State’s requirements and preferences. Data center encryption controls are confirmed in the SOC2 audit. Most intra-governmental calls via VoIP will be encrypted, and the State with the vendor is reviewing its IP phone deployment to identify any that do not support encryption. The Jabber client does support encryption. (Note: some calls do not support encryption, such as calls to 911 and calls to the conventional PSTN.)

11.6 WHAT FORMAT DOES THE VENDOR USE FOR CONTINUOUS VULNERABILITY MANAGEMENT, WHAT PROCESS IS USED FOR REMEDIATION, AND HOW DO THEY REPORT VULNERABILITIES TO CUSTOMERS?

The vendor’s Data Centers are Tier 3 rated or higher, with disaster recovery procedures tested as required for accreditation including SSAE-18 SOC1 Type 2 and SSAE-16 SOC2. These accreditations are consistent with the State’s requirements for secure cloud hosting. Additionally, it is the responsibility of NWN’s CSOT Team to perform routine vulnerability assessments of networked resources and evaluate for missing security patches. These assessments will be performed continuously to identify known vulnerabilities.

11.7 HOW DOES THE VENDOR DETERMINE THEIR COMPLIANCE MODEL AND HOW IS THEIR COMPLIANCE ASSESSED?

Please see 11.2 Data Classification, above.

12 RISK ASSESSMENT & RISK REGISTER

The risks identified throughout this review are collected below, along with an assessment of their significance, a description of the State response and timing, and our evaluation of the State response.

12.1.1 ADDITIONAL COMMENTS ON RISK

none

12.1.2 RISK REGISTER

Risk ID:	Identification number assigned to risk or issue.
Risk Rating:	An assessment of risk significance, based on multiplication of **(probability X impact ratings)** (*see below*). **1-9 = low** **10-48 = moderate** **49-90 high** See table below
Probability:	Assessment of likelihood of risk occurring, scale of **1,3,5,7, or 9**, from least to most likely
Impact:	Assessment of severity of negative effect, scale of **1,3,5,7, or 10**, from least to most severe
Finding:	Review finding which led to identifying a risk
Risk Of:	Nature of the risk
Source:	Project, Proposed Solution, Vendor or Other
Risk domains:	What may be impacted, should the risk occur
State's Planned Risk Strategy	Decision to *avoid*, *mitigate*, or *accept* risk
State's Planned Risk response	Detailed description of response to risk, in order to accomplish decision
Reviewer's Assessment:	Reviewer's evaluation of the State's planned response

Risk Rating Matrix			**IMPACT**				
			Trivial	Minor	Moderate	Major	Extreme
			1	3	5	7	10
LIKELIHOOD	Rare	1	1	3	5	7	10
	Unlikely	3	3	9	15	21	30
	Moderate	5	5	15	25	35	50
	Likely	7	7	21	35	49	70
	Very Likely	9	9	27	45	63	90

Risk ID: R1	Rating:	**9**	
	Likelihood:	**3**	
	Impact:	**3**	
Finding:	Conditions resulting from the ongoing Covid-19 pandemic could lead to restrictions on movement, social interaction, in-person working, or other aspects of implementation, interfering with work by State and/or vendor employees assigned to the project.		
Risk Of:	project delay, increased cost, inconsistent rollout of services		
Risk domains:	cost, project timeline		
State's Planned Risk Strategy:	The State accepts the risks. The State believes staying with the current vendor reduces risks as few implementation changes will be needed and all installation can be performed remotely.		
Reviewer Recommendation	none		
Reviewer's Assessment of State's Planned Response	concur		

Risk ID: R2	Rating:	**30**	
	Likelihood:	**3**	
	Impact:	**10**	
Finding:	The State intends an increased and continuing reliance on softphone clients, instead of acquiring many more standalone phones. Softphones may pose an inherently greater potential security risk, compared to standalone phones, when they are deployed on workstations that have access to other network resources. (See, for example, https://www.cisco.com/c/en/us/support/docs/csa/cisco-sa-jabber-ttcgB9R3.html). However, they are very inexpensive, are in wide use, meet many State needs, and most established clients such as Cisco are monitored for vulnerabilities.		
Risk Of:	security breach on desktop		
Risk domains:	security		
State's Planned Risk Strategy:	That State agrees with reviewer to mitigate by working with vendor, establishing best practices for softphone clients.		
Reviewer Recommendation	Mitigate: Rely on vendor experience and knowledge to develop appropriate best practices for those areas of software maintenance where the State has primary responsibility (e.g., maintaining softphone versions, identifying acceptable clients, and standardizing deployment)		
Reviewer's Assessment of State's Planned Response	concur		

Risk ID: R3	Rating:	**25**
	Likelihood:	**5**
	Impact:	**5**
Finding:	Knowledge about the State VoIP network is somewhat concentrated among a small number of long-term State personnel. Should those individuals become unavailable due to illness, retirements, or any other reason, implementation of a new system could be delayed.	
Risk Of:	implementation delay	
Risk domains:	project timetable	
State's Planned Risk Strategy:	The State agrees with the reviewer recommendation to mitigate this by cross training employees that are supporting this project. The business lead is already taking steps to do this from a contract management perspective and the network team also cross trains staff as best practices.	
Reviewer Recommendation	Mitigate: Identify relevant areas of concentration and assign appropriate employees to knowledge transfer activities such as shadowing, participation in meetings, shared research and activities, etc.	
Reviewer's Assessment of State's Planned Response	Concur	

Risk ID: R4	Rating:	**15**	
	Likelihood:	**3**	
	Impact:	**5**	
Finding:	The implementation of e911 services to some softphone clients (e.g., those installed on desktop workstations as opposed to those installed as mobile phone apps) require an additional software component "Sentry Gatekeeper" (supplied by the vendor) that requires location configuration and updating by the user. If the user is not adequately competent and/or diligent in location updating, the softphone client may be non-compliant with e911 rules (because it may not adequately reflect its geographic location). The State hopes to minimize this possibility by encouraging deployment of the mobile phone-based Cisco Jabber client (which automatically uses the host mobile phone location data for e911 location services).		
Risk Of:	e911 federal and State non-compliance for some softphone clients, liability for State if harm ensues		
Risk domains:	compliance, liability		
State's Planned Risk Strategy:	The State agrees with the reviewer's recommendations to mitigate the risk. In addition, the service desk currently sends out weekly notices to staff that are not in compliance with updating their location and requests them to set their address with instructions.		
Reviewer Recommendation	Mitigate: - Continue to maximize mobile phone client use. - Implement training and compliance check program for use of Sentry Gatekeeper - Implement clear policy for remote workers that includes e911 configuration compliance		
Reviewer's Assessment of State's Planned Response	Concur		

Risk ID: R4	Rating:	**3**	
	Likelihood:	**1**	
	Impact:	**3**	
Finding:	Statement of Work (SOW) in contract draft* refers to Contact Center implementation, but this implementation is out-of-scope for the project as currently envisaged.		
Risk Of:	inaccurate or confusing contract, project delay, miscommunication between vendor and State		
Risk domains:	contract, communication		
State’s Planned Risk Strategy:	The State does not wish to remove the Contact Center as this is an optional feature that the State may wish to take advantage of at some point over the contract term (5 years). The State's preference is to leave the commitment and pricing information in the contract and make sure that it is clearly identified as optional.		
Reviewer Recommendation	Mitigate: Remove Contact Center references from contract, or make clear that this portion is optional		
Reviewer’s Assessment of State’s Planned Response	concur		

13 ATTACHMENTS

Attachment 1 – Risk Register

Attachment 2 – Cost Spreadsheet

ATTACHMENT 2 - ENTERPRISE VOIP INDEPENDENT REVIEW -- Risk and Issues Register -- version 3.0.a 2021/May/30 -- Paul E. Garstki, JD -- Paul Garstki Consulting

RISKS	What is the finding that leads to identifying a risk? (This is a highly condensed version that is explained more fully in the report narrative)	What are the risks implied by the finding?	What aspects of the project are at risk if the risk(s) are realized?	What is the State's response to the risk?	What is the Independent Reviewer recommending? (The Reviewer does not necessarily make a recommendation for each risk)	Is the State's response to this risk adequate?	Latest the response should take place	Reviewer's assessment of likelihood risk is realized 1,3,5,7, or 10	Reviewer's assessment of impact if risk is realized 1,3,5,7, or10	1-9 low 10-48 medium
	Note: Risk ID # list may have gaps, in order to maintain consistency with earlier drafts									49-100 high
Risk #	**Finding**	**risk of**	**risk domains**	**SOV response**	**Reviewer Recommendation**	**Reviewer Assessment of SOV Response**	**Timing**	**likelihood 1-10**	**impact 1-10**	**total rating**
R1	Conditions resulting from the ongoing Covid-19 pandemic could lead to restrictions on movement, social interaction, in-person working, or other aspects of implementation, iinterfereing with work by State and/or vendor employees assigned to the project.	project delay, increased cost, inconsistent rollout of services	cost, project timeline	The State accepts the risks. The State believes staying with the current vendor reduces risks due as few implementation changes will be needed and all installation can be performed remotely.			ongoing	**3**	**3**	**9**
R2	The State intends an increased and continuing reliance on softphone clients, instead of acquiring many more standalone phones. Softphones may pose an inherently greater potential security risk, compared to standalone phones, when they are deployed on workstations that have access to other network resources. (see, for example, https://www.cisco.com/c/en/us/support/docs/csa/cisco-sa-jabber-ttcgB9R3.html). However, they are very inexpensive, are in wide use, meet many State needs, and most established clients such as Cisco are monitored for vulnerabilities.	security breach on desktop	security	That State agrees with reviewer to mitigate by working with vendor, establishing best practices for softphone clients.	Mitigate: Rely on vendor experience and knowledge to develop appropriate best practices for those areas of software maintenance where the State has primary responsibility (e.g., maintaining softphone versions, identifying acceptable clients, and standardizing deployment)		before implementation	**3**	**10**	**30**
R3	Knowledge about the State VoIP network is somewhat concentrated among a small number of long-term State personnel. Should those individuals become unavailable due to illness, retirements, or any other reason, implementation of a new system could be delayed.	implementation delay	project timetable	The State agrees with the reviewer reccomendation to mitigate this by cross training employees that are supporting this project. The business lead is already taking steps to do this from a contract management perspective and the network team also cross trains staff as best practices.	Mitigate: Identify relevant areas of concentration and assign appropriate employees to knowledge transer activities such as shadowing, participation in meetings, shared research and activities, etc.		during implementation	**5**	**5**	**25**
R4	The implementation of e911 services to some softphone clients (e.g., those installed on desktop workstations as opposed to those installed as mobile phone apps) require an additional software component "Sentry Gatekeeper" (supplied by the vendor) that requires location configuration and updating by the user. If the user is not adequately competent and/or diligent in location updating, the softphone client may be non-compliant with e911 rules (because it may not adequately reflect its geographic location). The State hopes to minimize this possiblility by encouraging deployment of the mobile phone-based Cisco Jabber client (which automatically uses the host mobile phone location data for e911 location services).	e911 federal and State non-compliance for some softphone clients, liability for State if harm ensues	compliance, liability	The State agrees with the reviewer's reccomendations to mitigate the risk. In addition, the service desk currently sends out weekly notices to staff that are not in compliance with updating their location and requests them to to set their address with instructions.	Mitigate: - Continue to maximize mobile phone client use. - Implement training and compliance check program for use of Sentry Gatekeeper - Implement clear policy for remote workers that includes e911 configuration compliance		ongoing	**3**	**5**	**15**

Attachment 1: Enterprise VoIP Cost Spreadsheet ver. 2.0a

Project Name:				Enterprise VoIP							Lifecycle Total @ Current Annual Cost	
Description	Qty	Unit Price	Monthly Price		Maintenance	Maintenance	Maintenance	Maintenance	Maintenance	Total		Benefit
Fiscal Year				Procurement	FY1	FY2	FY3	FY4	FY5			
HARDWARE												
Server Hardware				$ -	$ -	$ -	$ -	$ -	$ -	$ -		
Network Upgrades				$ -	$ -	$ -	$ -	$ -	$ -	$ -		
Desktop Hardware				$ -	$ -	$ -	$ -	$ -	$ -	$ -		
Other				$ -	$ -	$ -	$ -	$ -	$ -	$ -		
Hardware Total				**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**
Software												
Server Hardware				$ -	$ -	$ -	$ -	$ -	$ -	$ -		
Network Upgrades				$ -	$ -	$ -	$ -	$ -	$ -	$ -		
Desktop Hardware				$ -	$ -	$ -	$ -	$ -	$ -	$ -		
Other				$ -	$ -	$ -	$ -	$ -	$ -	$ -		
Software Total				**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ 375,000.00**	**$ 375,000.00**
SERVICES												
VOIP SERVICES												
Ongoing Monthly Service Costs												
UC Subscription – Common Area (Qty 500)	**500**	**$ 5.65**	**$ 2,825.00**	$ -	$ 33,900.00	$ 33,900.00	$ 33,900.00	$ 33,900.00	$ 33,900.00	$ 169,500.00		
UC Subscription – Named User (Qty 4,478)	**4478**	**$ 8.15**	**$ 36,495.70**	$ -	$ 437,948.40	$ 437,948.40	$ 437,948.40	$ 437,948.40	$ 437,948.40	$ 2,189,742.00		
UC Subscription – Personal Video Device (Qty 6)	**6**	**$ 8.80**	**$ 52.80**	$ -	$ 633.60	$ 633.60	$ 633.60	$ 633.60	$ 633.60	$ 3,168.00		
UC Subscription – MultiPurpose Video Device (Qty 16)	**16**	**$ 46.50**	**$ 744.00**	$ -	$ 8,928.00	$ 8,928.00	$ 8,928.00	$ 8,928.00	$ 8,928.00	$ 44,640.00		
UC Subscription – Emergency Responder (Qty 5,000)	**5000**	**$ 1.30**	**$ 6,500.00**	$ -	$ 78,000.00	$ 78,000.00	$ 78,000.00	$ 78,000.00	$ 78,000.00	$ 390,000.00		
SBC and Geo-Redundant Infrastructure for 25k Devices (Qty 1)	**1**	**$ 1,290.00**	**$ 1,290.00**	$ -	$ 15,480.00	$ 15,480.00	$ 15,480.00	$ 15,480.00	$ 15,480.00	$ 77,400.00		
Additional Features/Functions												
Private 50Mb Circuits (2)	**2**	**$ 785.00**	**$ 1,570.00**		$ 18,840.00	$ 18,840.00	$ 18,840.00	$ 18,840.00	$ 18,840.00	$ 94,200.00		
Local and Long Distance Service for US, Canada and Mexico (5,000)	**5000**	**$ 0.95**	**$ 4,750.00**		$ 57,000.00	$ 57,000.00	$ 57,000.00	$ 57,000.00	$ 57,000.00	$ 285,000.00		
E911 Enabled DID (5,000)	**5000**	**$ 0.25**	**$ 1,250.00**		$ 15,000.00	$ 15,000.00	$ 15,000.00	$ 15,000.00	$ 15,000.00	$ 75,000.00		
Taxes, Fees, Federal Surcharges, etc.												
Federal USF (Jan 2020 rate = 21.1%)	**1**	**$ -**	**$ -**		$ 15,125.16	$ 15,125.16	$ 15,125.16	$ 15,125.16	$ 15,125.16	$ 75,625.80		
E911 and CRF fees (Dec 2019 rate = 4.3%)	**1**	**$ -**	**$ -**		$ 3,082.38	$ 3,082.38	$ 3,082.38	$ 3,082.38	$ 3,082.38	$ 15,411.90		
	0	**$ -**	**$ -**		$ -	$ -	$ -	$ -	$ -	$ -		
											$ 5,105,053.50	
CONTACT CENTER SERVICES												
Implementation (Contact Center)												
Contact Center Platform Build and Configuration				$ -	$ -	$ -	$ -	$ -	$ -	$ -		
Telecommunications equipment/circuits				$ -	$ -	$ -	$ -	$ -	$ -	$ -		
Hardware (Operational Purchase Option)				$ -	$ -	$ -	$ -	$ -	$ -	$ -		
Phone Lease Option (Price per Device per month) (Qty 1,125)	**0**	**$ 2.32**	**$ -**		$ -	$ -	$ -	$ -	$ -	$ -		
Ongoing Monthly Service Costs (Contact Center)												
Contact Center Agent (Qty 300)	**0**	**$ 59.00**	**$ -**		$ -	$ -	$ -	$ -	$ -	$ -		
Contact Center Supervisor with QM (Qty 51)	**0**	**$ 73.00**	**$ -**		$ -	$ -	$ -	$ -	$ -	$ -		
Call Center Features from Section 3 of RFP (351 Agents)	**0**	**$ 35.50**	**$ -**		$ -	$ -	$ -	$ -	$ -	$ -		
UC Subscription – Common Area (Qty 0)	**0**	**$ 5.65**	**$ -**		$ -	$ -	$ -	$ -	$ -	$ -		
UC Subscription – Named User (Qty 351)	**0**	**$ 8.15**	**$ -**		$ -	$ -	$ -	$ -	$ -	$ -		
Telecommunication Charges (Contact Center)	`											
Local and Long Distance Service plus DID for Contact Center (Qty 1)	**0**	**$ 9,450.00**	**$ -**		$ -	$ -	$ -	$ -	$ -	$ -		

Taxes, Fees, Federal Surcharges, etc. (contact Center)												
Federal USF (Jan 2020 rate = 21.1%)			$ -		$ -	$ -	$ -	$ -	$ -	$ -		
E911 and CRF Fees (Dec 2019 rate = 4.3%)			$ -		$ -	$ -	$ -	$ -	$ -	$ -		
PUBLIC SAFETY SERVICES												
Implementation (Public Safety)												
Public Safety Migration				$ 19,500.00						$ 19,500.00		
Telecommunications equipment/circuits				$ 1,290.00	$ 15,480.00	$ 15,480.00	$ 15,480.00	$ 15,480.00	$ 15,480.00	$ 78,690.00		
Hardware (Operational Purchase Option)				$ 165.89	$ 15,125.16	$ 15,125.16	$ 15,125.16	$ 15,125.16	$ 15,125.16	$ 75,791.69		
Phone Lease Option (Price per Device per month) (Qty 1,125)	1125	$ 2.32	$ 2,610.00		$ 31,320.00	$ 31,320.00	$ 31,320.00	$ 31,320.00	$ 31,320.00	$ 156,600.00		
Ongoing Monthly Service Costs (Public Safety)												
Small Survivable Site (1 – 50) (Qty 12) Up to 4 POTS / 50 Devices	12	$ 285.00	$ 3,420.00		$ 41,040.00	$ 41,040.00	$ 41,040.00	$ 41,040.00	$ 41,040.00	$ 205,200.00		
Medium Survivable Site (51 – 200) (Qty 2) Up to 16 POTS / 200 Devices	2	$ 425.00	$ 850.00		$ 10,200.00	$ 10,200.00	$ 10,200.00	$ 10,200.00	$ 10,200.00	$ 51,000.00		
Large Survivable Site (201 – 500) (Qty 1) Up to 2 PRI / 500 Devices	1	$ 560.00	$ 560.00		$ 6,720.00	$ 6,720.00	$ 6,720.00	$ 6,720.00	$ 6,720.00	$ 33,600.00		
UC Subscription – Common Area (Qty 77)	77	$ 5.65	$ 435.05		$ 5,220.60	$ 5,220.60	$ 5,220.60	$ 5,220.60	$ 5,220.60	$ 26,103.00		
UC Subscription – Named User (Qty 697)	697	$ 8.15	$ 5,680.55		$ 68,166.60	$ 68,166.60	$ 68,166.60	$ 68,166.60	$ 68,166.60	$ 340,833.00		
Telecommunication Charges (Public Safety)												
Local and Long Distance Service plus DID for Public Safety (Qty 774)	774	$ 1.20	$ 928.80		$ 11,145.60	$ 11,145.60	$ 11,145.60	$ 11,145.60	$ 11,145.60	$ 55,728.00		
Taxes, Fees, Federal Surcharges, etc. (Public Safety)												
Federal USF (Jan 2020 rate = 21.1%)					$ 2,351.72	$ 2,351.72	$ 2,351.72	$ 2,351.72	$ 2,351.72	$ 11,758.60		
E911 and CRF Fees (Dec 2019 rate = 4.3%)					$ 479.26	$ 479.26	$ 479.26	$ 479.26	$ 479.26	$ 2,396.30		
											$ 394,500.00	
Service Total				$ 20,955.89	$ 891,186.48	$ 891,186.48	$ 891,186.48	$ 891,186.48	$ 891,186.48	$ 4,476,888.29		$ 1,022,665.21
Consulting Services												
Independent Review				$ 24,982.00						$ 24,982.00		
										$ -		
Consulting Total				$ 24,982.00	$ -	$ -	$ -	$ -	$ -	$ 24,982.00	$ -	$ (24,982.00)
Training												
										$ -		
Other				$ -	$ -	$ -	$ -	$ -	$ -	$ -		
Training Total				$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -
Implementation Services												
EMP Platform Migration	1	$ 3,750.00		$ 3,750.00						$ 3,750.00		
E911 Solution	1	$ 28,200.00		$ 28,200.00						$ 28,200.00		
Implementation Services Total				$ 31,950.00	$ -	$ -	$ -	$ -	$ -	$ 31,950.00	$ -	$ (31,950.00)
Personnel - Additional												
State Personnel												
ADS VoIP Staff				$ -	$ 303,011.31	$ 303,011.31	$ 303,011.31	$ 303,011.31	$ 303,011.31	$ 1,515,056.55	$ 1,951,856.55	
ADS EPMO Project Oversight & Reporting				$ 27,456.00						$ 27,456.00		
ADS EPMO Project Manager for Implementation				$ 183,040.00						$ 183,040.00		
ADS Enterprise Architect Staff for Implementation				$ 9,240.00						$ 9,240.00		
ADS Security staff for Implementation				$ 24,140.00						$ 24,140.00		
Other ADS IT Labor for Implementation				$ 150,000.00	$ -	$ -	$ -	$ -	$ -	$ 150,000.00		
				$ -	$ -	$ -	$ -	$ -	$ -	$ -		
Personnel - Additional Total				$ 393,876.00	$ 303,011.31	$ 303,011.31	$ 303,011.31	$ 303,011.31	$ 303,011.31	$ 1,908,932.55	$ 1,951,856.55	$ 42,924.00
Grand Total				$ 471,763.89	$ 1,194,197.79	$ 1,194,197.79	$ 1,194,197.79	$ 1,194,197.79	$ 1,194,197.79	$ 6,442,752.84	$ 7,826,410.05	$ 1,383,657.21