Independent Review

of the

HOSTED COLOCATION DATA CENTER SPACE PROJECT

for the

State of Vermont

Department of Information and Innovation

Submitted to the

State of Vermont, Office of the CIO

By

Northeast Computer Systems, Inc.
602 Main St.
Lyndonville, VT 05851

January 8, 2013

prepared by: Paul E. Garstki

Preface

The analysis was based on the materials provided by

Martha Haley, Project Manager, DII

Michael Morey, Chief Technology Officer, DII

Joe Ng , Data Center Mainframe Operations Director, DII

Steve Bentley, Information Technology Manager, AHS

These individuals were interviewed by Paul E. Garstki, from NCS. Follow-up questions were answered by the individuals above, and

Peter Kipp, Contracts and Procurements Specialist, DII

Peter Jaquith, Interim Network Manager, DII

Scott Pierce, COO, Tech Vault

Thanks to Martha Haley for gathering all the initial documents for review, and for facilitating quick and helpful communication throughout. All participants were entirely helpful and forthcoming throughout this process.

CONTENTS

Executive Summary

Summary of Key Points

Acquisition cost assessment	• One-time costs for the project total approximately **$670,000**. • Annual costs for the project total approximately **$556,000**, based on current prices.
Technology architecture	Moving the equipment contained in certain State data centers into a state-of-the-art hosted facility essentially upgrades the security, reliability, and recoverability of that part of the State's data infrastructure. This project is a sub-project of I-TOP, and is therefore consistent with State IT Strategic Direction.
Assessment of Implementation Plan	The Implementation Plan (Project Management Plan) is comprehensive and well-thought-out. The project contains a number of sub-projects, but as long as Project Team maintains a high level of communication and continues as planned, any risks will be avoided or well-mitigated.
Assessment of Implementation Contractor	The selected vendor, Tech Vault, is the good and obvious choice in terms of services offered, quality, and value. Any questions about financial stability should be resolved through due diligence by the State during the contract negotiation process.
Cost/benefit analysis	Project represents a net improvement to State data infrastructure; it is not implemented as a cost savings plan. However, project costs are contained within existing operational budget.
Risk Management Plan	Few risks. Risks have high impact, but very low likelihood of realization.

KEY ISSUES

The key issues and concerns are few. This is a complex project insofar as it contains several sub-projects that must be completed before the move can take place. However, the project and its sub-projects are extremely well planned. As long as communication within the Project Team remains at a high level, and the Project Management Plan is adhered to and modified as new information arises, we expect that the likelihood of realization for all identified risks will be low (see Risk Management Plan, below).

RECOMMENDATION

We recommend that the State continue this project with the selected vendor, Tech Vault, as laid out in the Project Management Plan.

Overview of this Document and Background

Scope of this Independent Review

This document fulfills the requirements of Vermont Statute, Title 3, Chapter 45, §2222(g):

> *The secretary of administration shall obtain independent expert review of any recommendation for any information technology activity initiated after July 1, 1996, as information technology activity is defined by subdivision (a)(10) of this section, when its total cost is $500,000 or greater. Documentation of such independent review shall be included when plans are submitted for review pursuant to subdivisions (a) (9) and (10) of this section. The independent review shall include:*
>
> - *an acquisition cost assessment;*
> - *a technology architecture review;*
> - *an implementation plan assessment;*
> - *a cost analysis and model for benefit analysis; and*
> - *a procurement negotiation advisory services contract.*

The art and practice of Information Technology Project Management (IT PM) has evolved significantly since the passage of Section 2222(g) in the mid-1990's. In order to enhance the usefulness of this review in the context of IT PM advancements, while remaining true to the spirit of the legislation, this review also includes a Risk Management Plan, identifying key risks to the Project as seen at the time of review, along with specific plans for mitigation and/or avoidance of the occurrence of those risks.

DII Data Center Colocation Project Historical Background

As the State continues with its consolidation of physical IT equipment and virtualization projects, the need for appropriate physical space and power to support data center needs will continue to grow in the very near term. The State anticipates that, sometime in or shortly after 2013, this expansive need will peak. Thereafter, the success of virtualization and the probable increase of cloud based solutions to State IT needs will begin to *reduce* the need for physical space and power, probably over a 5-10 year period.

This project is in direct response to this needs estimate growing out of the State's strategic systems direction, coupled with a recognition that current State data center facilities (both owned and leased) fall short of meeting state-of-the-art requirements in a number of ways, including physical robustness and security, power supply, redundancy, and disaster avoidance/recovery. The State faces a choice in responding to this analysis. It may either:

1. Upgrade existing facilities; or,
2. Build new facilities; or,
3. Lease space and services in hosted facilities that meet these needs; or,
4. Employ some combination of the above.

The State has concluded that it may not choose to do nothing about the above analysis, because

- The consolidation project will fill currently available space
- Some current facilities present an increased risk of potentially catastrophic data loss, because they either do not, or will not continue to, meet industry standards for security, robustness, and disaster recovery.

We wholeheartedly agree.

Each of the first 3 alternatives has some drawbacks. These drawbacks may be summarized as follows:

Upgrade existing facilities:

> Many existing facilities are small, geographically dispersed, and are adapted from structures not purpose-built as data center facilities. Wholesale upgrade of these facilities would be expensive because of duplication, and could not address all of the problems inherent in their designs and locations. However, it may be necessary to upgrade some facilities as a "stopgap" measure.

Build new facilities:

Building new data centers to state-of-the-art specifications would entail considerable expense. (A new primary data center might cost $10 million.) While the State could decide to pursue this route – for example, by means of a bond issue – the drawback is that the current estimate expects the need for capacity to *diminish* after the initial expansion phase. The State could, therefore, find itself in possession of excess capacity, both in terms of physical space and supporting staff employment, perhaps in a 6-12 year time span. When the capacity was no longer needed, it would have to be discarded, perhaps while the bond issue was still being paid back. This seems a less-than-ideal solution, although it is not "off the table."

Lease space in hosted facilities:

Using a hosted facility obligates the State to significant operational costs in a direction it has not previously pursued *at this level of quality*. Vermont has few hosting facilities that meet state-of-the-art specifications, and a facility located outside the state could introduce problems of latency, cost of servicing, and supervision.

Upon consideration, and especially given the analysis of initial expansion followed by relatively rapid contraction of data center needs, the State decided that the best course of action was to pursue the use of hosted facilities. Initial cost outlay would be minimal, compared to construction of a new facility, and the need to expand an internal technical staff with state-of-the-art data center qualifications could be avoided. Perhaps most significantly, the State will not be "caught" by the contraction phase of the growth cycle, with its resultant decrease in needs for physical data center facilities *and* qualified staff.

Deciding upon a 2-prong plan of action, the State released 2 simultaneous RFPs: one for a primary data center, and one for a secondary data center. From the outset, these 2 RFP's were designed to be separable. Requirements, apart from size of the facilities and desired physical location, were similar for both RFP's. No single vendor could be selected for both proposals simultaneously (although vendors were allowed to bid on both). External engineering expertise (Leading Edge Design Group) was engaged to assist in defining data center requirements and designing the RFP.

The low number of qualified responses for the primary data center RFP resulted in a decision to select a vendor only for the secondary data center.

The project will relocate two data centers – at McFarland in Barre and on Cherry Street in Burlington – to the secondary hosted data center in Williston

Three responding vendors were chosen as finalists in the selection process. Once again, external expertise in the form of Leading Edge Design Group was employed to assist in evaluating the finalist vendors, eliciting further information, conducting site visits, and developing a scoring matrix that might be used to make a final selection. Chief Technology Officer Michael Morey, and Data Center Mainframe Operations Director Joe Ng adapted and expanded that scoring matrix to select the vendor. They each scored the vendors independently and then compared results to make a final decision. Apparently, their independent scores were highly consistent with each other.

Tech Vault was selected as the project vendor on the basis of overall quality of offering, price, and consistency with State needs.

Some Comments on Choice of Vendor and Vendor Stability

In the context of this review, we concur that Tech Vault represents the obvious choice in terms of services offered, quality, and value. Regardless, we wish to note two perceived risks which should be addressed by the State before a contract is executed.

1. Vendor will not release detailed financials

The State prefers vendors to disclose financial details of their business operations, in order to evaluate the financial stability of the vendor. Tech Vault declined to reveal such details (as a close corporation). They did, however, point to a 25% ownership stake by ICV, as some evidence of financial resources.

An example of a question that might be difficult to answer without adequate financial data: Would the vendor be able to continue complete service to the State in the event that vendor loses a large current customer?

If vendor is not adequately funded, it could fail to perform adequately, or fail completely, even if highly motivated.

We are told that it is increasingly common for close corporations and privately held companies to decline to release financials when negotiating with the State. The State reserves the right to be flexible in its RFP/RFQ response evaluations and may decide to select a vendor without this data. At the same time, it is likely that this project team has been focused more on the technical performance of the vendor than on financial stability.

We recommend that some time be set aside to focus on this issue in collaboration with the appropriate State legal and financial resource persons.

2. Vendor's corporate structure may be somewhat unusual in a large contract

Tech Vault is organized as a Sub Chapter S corporation (Vermont), a structure usually associated with smaller business concerns. This may be somewhat unusual if the State commonly deals with large corporations organized as Sub Chapter C corporations, and/or publicly held corporations.

Tech Vault has no employees. The facility is operated and managed by the employees of Tech Group, Inc., an affiliated corporation with a common ownership to that of Tech Vault.

The State must be able to seek appropriate remedies in the event of injury.

We are not stating that there is anything wrong or inappropriate about Vendor's corporate structure. We are not making a legal statement, but only noting that this structure (S corp, with all employees from an affiliate) may be unusual for the State to encounter in a large contract.

We recommend that the State's legal and financial experts through due diligence satisfy themselves that this structure does not expose the State to undue risk in the event of sub-par performance.

Limitations of this Review

As noted below, this Project includes several sub-projects, such as build-out of dark fiber, acquisition of network gear, and moving of mainframe. As the details of some of these sub-projects will be determined largely after the Tech Vault contract is executed, we could review only the general outlines of these plans to assure ourselves that there is little likelihood of risk.

Project Goal

Data Centers currently at McFarland in Barre and on Cherry Street in Burlington will be moved to a hosted data center meeting stringent specified requirements, in order to enhance security, reliability, and recoverability without decreasing performance.

Project Scope

*From: **SOV Hosted Data Center Abbreviated Project Charter**, v.2.0, 11/20/2012*

The scope of this project includes and excludes the following items:

In Scope:

1. Select and contract with a Host Data Center Provider that will meet the following requirements:
    a. Facility Security, Dedicated Space, and Data Security: The State requires a facility that is highly secure with separate levels and multiple points of authentication. The State requires a dedicated suite for their data center. The suite shall be separately secured with electronic access. All cabinets located inside the suite shall be independently secured.
    b. Racks & IT Load: The State requires data center space in their dedicated suite for 10 -15 contiguous racks, inclusive of 4 (four) cabinets for mainframe equipment. The total anticipated IT load at full build out is estimated to be between 100kW – 200kW.
    c. Access: The State requires 24/7/365 access to the data center facility.
    d. Availability: The State requires a highly available data center facility that offers redundancy in critical infrastructures including (but not limited to): mechanical, electrical, telecommunications.
    e. Energy Efficiency: The State seeks a highly efficient data center facility that leverages innovative technology and the favorable environmental conditions in Vermont to reduce energy consumption in the data center.
    f. Enclosure & Finishes: The State requires a well designed and constructed, industry-compliant data center envelope with appropriately selected materials

for flooring, paints, ceilings, insulation, wall construction, etc. that are consistent with industry standards and best practices.

g. Fire Suppression: The State requires clean agent as the fire suppression mechanism in the data center.
h. Industry Standards: The State seeks a data center compliant with industry standards as defined by (but not limited to) the following organizations: ASHRAE, NEC, NFPA, BICSI, IEC, The Uptime Institute, The Green Grid, TIA/EIA, US Department of Energy.
i. Certifications: The State seeks a data center that will allow the state to meet certification requirements such as: SAS 70, SSAE 16, ISO 27002, PCI, HIPAA.

2. Purchase equipment needed (network and equipment to go inside the Data Center) for the Hosted Data Center.
3. Shut-down the McFarland (Barre) and Cherry Street (Burlington) Data Centers. Move the needed mainframe equipment, and reinstall the equipment at the Hosted Data Center site.
4. Shutdown the South Burlington co-location Level 3 facility
5. Get the data circuit in place to support network connectivity.
6. Ensure the Hosted Data Center is built to accommodate future SOV growth needs (i.e., the potential for consolidating more of the state's Data Centers at the hosted site).

Out of Scope**:**

1. Consolidating the remaining Data Center sites in the State of Vermont environment
2. Anything else not identified in the "In Scope" section above

DELIVERABLES PRODUCED:

Deliverable 1	Documents to Support SOV Project Management (Project Charter, Project Plan, Communication Plan, Issue Log, etc.)
Deliverable 2	Contract with Hosted Data Center Provider (contract to include SLA, Preventive Maintenance & Disaster Recovery Plan)
Deliverable 3	Project Plan from Host Site Contractor
Deliverable 4	Business Requirements (for both Contractor & SOV work)
Deliverable 5	SOV Equipment Bid & Order (network gear for hosted site)
Deliverable 6	Contract with IBM for Mainframe computer moves & installation
Deliverable 7	Contractor Site Design Plan
Deliverable 8	SOV Network Design Plan
Deliverable 9	Test Plan (Site & Network)
Deliverable 10	Moving/Installation Plan (includes Schedule of Move Events, Contingency Plan, Install Success Verification Plan, etc.)
Deliverable 11	Fully Tested & Implemented Hosted Site

Acquisition Cost Assessment

This chapter reviews the stated costs of in scope project activities. Salaries or wages of current State employees participating in project activities are not included. Note that this project includes a number of sub-projects (moving mainframe computer, building out dark fiber, bidding out needed network equipment) some of which are necessarily estimates at this point. However, there is a high confidence that the estimates are realistic.

This project represents a net improvement to State data infrastructure; it is not implemented as a cost savings plan. However, project costs are contained within existing operational budget. State employees operating, monitoring, or otherwise managing equipment that will be moved will continue to operate equipment in the new location. Any new needed personnel for operating the data center facility *per se* (as opposed to the State's equipment hosted within it) are provided by vendor Tech Vault as included in monthly charges.

Cost of Hardware

One Time Costs

- Network Equipment: Moving existing servers into the hosted data center facility will entail the acquisition of network gear to contain, connect, and integrate the servers with the new rack environment. A separate RFQ has been developed for this equipment; which is, however, a component of the present project. Total capital cost for this network equipment is estimated to be **$475,000**.
- Build-out of the dark fiber circuit that will connect the hosted equipment to the State's access point is estimated to cost **$140,000**. Exact cost will depend upon final specifications.

Recurring Costs

- (see *Maintenance contracts and replacement costs for 5-6 year life cycle* in **Annual Costs**, below)

Cost of Software

- N/A

Cost of Services

One-Time Costs

- IBM mainframe move: **$25,000**.
- Professional move services for other equipment: **$25,000**.
- Move Level 3 connection: **$5,000**.

Annual Costs

- Co-location estimate (rack charges + power): $25,000 / mo., **$300,000 / year**.
- Dedicated circuit: $96,000 / year.
- Maintenance contracts and 5-6 year life cycle replacement costs for network gear is estimated to cost **$160,000 / yr.**

System Integration Costs

- N/A

Additional Costs

- none identified

Summary

- One-time costs for the project total approximately **$670,000**.
- Annual costs for the project total approximately **$556,000**, based on current prices.

TECHNOLOGY ARCHITECTURE REVIEW

This chapter reviews the appropriateness of the project technology, in the context of the current state of the art, as well as in light of the State's current Strategic Systems Direction. The purpose is to ensure that the project represents a net move forward for the State's IT footprint, avoiding the creation of any significant new problems while attaining the project goal.

STATE OF THE ART

In developing this project, the State chose to specify a data center hosting facility meeting requirements that may be said to be "state of the art." Specifically, industry standards and certifications were noted (see Project Scope, above) and required in the RFP. In addition, the State set requirements for Security, Design, Access, Availability, Energy Efficiency, Fire Suppression, Fit and Finish, and Safety, which meet current industry standards for new facilities, and represent an enormous step forward in comparison to the State owned or leased facilities that are being replaced.

SUPPORT FOR THE STATE'S STRATEGIC ENTERPRISE SYSTEMS DIRECTION

This project is a sub-project of the State of Vermont Information Technology Optimization Project (ITOP), a main component of the State's Strategic Enterprise Systems Direction. As such, the project under consideration is inherently in support of that direction.

SECURITY ANALYSIS:

As part of the original RFP, significant security targets consistent with industry standards were identified, with vendors required to respond with details of how such targets are met. Tech Vault claims to meet SSAE-16 audit requirements, and personal investigation and on-site visits from State personnel confirm that the facility appears to be highly secure physically. Furthermore, remote monitoring capabilities are extensive and appropriate.

While we agree that Tech Vault appears to be a state-of-the-art facility in security terms, we also note that the facility does not have security personnel continuously on site. We believe it is important for the State to recognize the nature of physical security at an unpopulated site, and to enhance training of State personnel to avoid any compromise of strict security protocols, such as bringing unauthorized guests into the facility (which admittedly may be difficult but not impossible).

Joe Ng , Data Center Mainframe Operations Director, will be responsible for designing security protocols on the State side. He agrees with the above assessment, and has written,

> *Access to SOV Data Center at Tech Vault will be more restrictive, since there will be very limited # of people who will have access to this facility. In*

addition, there will be 2 form of authentication (Card key and access code) for gaining access. This facility should enable us to improve access control. We will also maintain sign-in sheets (IRS regulation) in our facility for people who are authorized but do not have access badge, such as vendor performing maintenance. We plan to escort anyone who is not authorized to access the data center alone. Currently, there is no formal security training. However, with the new security implementation at Tech Vault, we expect new security training is needed for this facility.

We continue to identify security issues as a risk for a remote, personally unattended facility. However, we believe the State's response is appropriate; given the high cost of human security personnel, such facilities are likely to become more common in the future, and developing appropriate procedures will help to ensure that they remain as secure as is feasible.

In passing, we note that several people both from the State and from Tech Vault have mentioned the proximity of the South Burlington Police building at 200 feet from the Tech Vault facility. While this *might* mean that police respond quickly to an emergency when called, we point out that it certainly does not mean that the facility is somehow monitored by the police. We doubt that the police wish the public to evaluate safety in terms of distance from a police station. It would probably be best not to consider this as a significant metric of security.

Disaster Recovery Plan

The Tech Vault facility employs redundant technology and comprehensive disaster recovery plans.

It is also important for the State to have adequate DR plans in place for the equipment moving phase of this project. The moving of equipment on the "move day(s)" will involve physically disconnecting, carrying across town, reconnecting, and restarting equipment, some of which carries production data. During this sequence, there is probably a greatly increased risk that some misfortune may damage one or more servers, or the data contained therein. The Project Management Plan already includes a path to a contingency plan, but has not yet reached the point of realization.

Temporarily lost data and/or down equipment would create delays impacting State employees and, to some extent, members of the public who access AHS web sites. Permanently lost data could incur additional costs.

As long as recovery and restoration procedures exist, backups are current, and the equipment is known to be replaceable, any data loss should be temporary. Therefore, we recommend that the Contingency Plan, as it is developed, will include identification and review of these procedures for all moved servers, and creation of such procedures wherever they do not already exist. Any technicians involved in the move should have access to these procedures readily available.

We understand that

- Many servers are already virtualized, simplifying the recovery plan(s)
- There is one DEC Alpha server (Cherry St.) which may not be easily replaceable, because of its age. There should be some plan for what to do if this server is damaged in the move.
- The mainframe equipment will be moved by IBM and the above issues are assumed to be addressed for the mainframe

State-wide WAN Impact

This project does not involve a net change to volume of traffic in the State-wide WAN. Moving some servers (i.e., Cherry Street AHS servers in Burlington) to a location more distant from some of the user base raises the *possibility* of latency issues. The project includes an upcoming analysis and test of latency issues during the design and implementation phases of the fiber build-out. This should address any negative issues that arise.

In a larger sense, the move to a state-of-the-art facility should result in an improvement to State WAN operations, with greatly improved monitoring and a signal path designed from the ground up.

System Integration Requirements

N/A

LAN Impact

N/A

Information Technology Server Optimization Plan

See *Support for the State's Strategic Enterprise Systems Direction*, above.

Ability of the Technology to Support Business Needs

This project moves servers which host the following applications:

- Mainframe Failover environments (All AHS, TAX, DMV) mainframe applications
- Peoplesoft Financials/Human Resource Failover environments
- SOV Private Cloud failover environments
- AHS systems like file services, citrix, and some odds and end applications that are now being served from Cherry Street.

A large number of servers in the non-mainframe environments have already been virtualized. This project does not include changes to the servers themselves. The users of these applications will likely notice no significant differences after the move is complete. However, the security, reliability, and recoverability of the applications on many of these servers will have been greatly enhanced. The end result is a greatly reduced risk of downtime or data loss.

Ability of the User and Operational Staff to Integrate Solution into their Work

As stated just above, the user base will not likely notice differences in operation once the project is completed.

The Security Analysis, above, refers to enhancements of the training process and supervision for State employees who must physically access the hosted data center facility. These are common improvements in the industry, and State employees will expect and even welcome them.

Summary

This project is a sub-project of the State of Vermont Information Technology Optimization Project (ITOP), a main component of the State's Strategic Enterprise Systems Direction. As such, the project under consideration is inherently in support of that direction.

We point out that with the employment of a remote hosted SSAE-16-audited data center, the State moves into a new level of physical security, made more challenging by the absence of continuous on-site staffing. The State will need to review and enhance its oversight and training procedures for State employees who need to access the data center.

It is also important for the State to have adequate disaster recovery plans in place for all of the equipment moved in this Project.

ASSESSMENT OF IMPLEMENTATION PLAN

This chapter assesses the Project Management Plan for appropriateness of the timeframe and adequacy of planning resources for the Project. We also briefly assess the readiness of State personnel to implement the Project.

Note about the RISK MANAGEMENT PLAN in Appendix 3

> In order to enhance the usefulness of this review for the purpose of Project Management, this review also includes a Risk Management Plan, in the form of a Risk Register, found at Appendix 3 – Risk Management Plan. In the Register we identify and evaluate key risks to the Project as seen at the time of review, along with specific plans for mitigation and/or avoidance of the occurrence of those risks, and individuals who will implement the plans.
>
> Throughout the present review document, risks of various sorts are identified and explained. These risks have been collected and tabulated, and they correspond one-to-one with risks in the Risk Register.

THE REALITY OF THE TIMETABLE

While this project focuses on the selection of Tech Vault as the vendor for the data center colocation facility, it also encompasses several sub-projects, such as

- Moving of mainframe facility (by IBM)
- Planning network expansion and build-out of fiber
- acquisition of network gear / building and preparation of new racks

In order for the project to go smoothly, the sub-projects must be completed by the designated "move days." This could be difficult as several vendors will be involved, and several individuals will supervise the sub-projects.

If one or more sub-projects are not ready by "move day," the date might be postponed. The State might incur some concurrent costs for overlapping services, negotiated and/or communicated "windows of opportunity" could be missed, causing distress for some State employees or the general public (i.e., those who access AHS web sites).

The State has chosen to deal with this issue by adopting a sufficiently long lead time for the sub-projects to mature. Since there is little risk in the projects coming to completion too soon (with the possible exception of "turning on" Internet connectivity before it is needed). This should be an adequate response.

However, it is important that communication throughout the project team about the status of sub-projects and any change in their respective time frames continues throughout.

TRAINING OF USERS IN PREPARATION FOR IMPLEMENTATION

(*NOTE: This point is addressed in the* ***Security Analysis****, above.)*

READINESS TO PARTICIPATE

This project has an *extremely* high degree of ownership and participation among team members. The basic idea of using a hosted data center provider has been discussed and analyzed within DII for some years.

ADEQUACY OF DESIGN, CONVERSION, AND IMPLEMENTATION PLANS

This project was developed and is being managed within the Department of Information and Innovation (DII). As such, Project Management is handled directly by the PM Office, and there is no Oversight Project Manager (as there would be for a project of another State Agency).

The Project Management Charter and Plan is very clear and reasonably extensive. While much of the project has yet to be realized (see *The Reality of the Timetable,* above), the defined tasks are well-defined, clearly documented, and appropriately resourced. As long as internal communication and project refinement continues as it has so far, we anticipate no issues with Project Management.

Adequacy of Support for Conversion and Implementation Activities

Several of the Project Team members (e.g., Michael Morey, Joe Ng, Peter Jacquith, and others) are also key personnel in the day-to-day operations of the Department of Information and Innovation, with responsibilities going far beyond the implementation activities of this project. We note with approval that these team members are adequately delegating project responsibilities to their respective staffs. It will be essential for team members to continue to delegate tasks to avoid any danger of project delay due to individuals' scheduling problems.

Adequacy of Department and Partner Staff to Provide Project Management

This project is managed by Project Manager Martha Haley, a highly skilled and certified professional. Team members on this project praise Martha's skills in organizing the project and the team, keeping communication current, and organizing project documentation.

We note without criticism that Ms. Haley's knowledge and experience of the *specific hosted data center technologies* of this project are not extensive. In a *different* environment, if project team members deferred to the Project Manager for technology decisions (such as timing issues between sub-projects), the risks of timing issues might increase. As it happens, ownership of this project is at such a high level, and support for the Project Manager's role so clear, that we have no hesitation in stating that the project is well-staffed.

Adequacy of Planned Testing Procedures

In a service-based project such as this, the Service Level Agreement (SLA), negotiated between vendor and the State, defines the expected levels of service and the remedies that will make good any shortfalls. This is similar to acceptance testing, except that the time frame for testing is ongoing and continuous. Various monitoring systems are or will be available, both on the vendor side and the State side. Data Center Mainframe Operations Director Joe Ng is satisfied with the remote monitoring systems that will be available to him. As in other aspects of this project, they represent a significant advancement over what is currently available to remotely monitor State data center sites.

The Service Level Agreement

It has been stated that the project team has light experience in developing an SLA *for a hosted data center project*. Contract negotiations could be delayed if development of an SLA is slow. In a *worst case scenario*, the result could be an incomplete and inadequate SLA that puts the State at risk for downtime, data loss, additional expense, or legal action in the event of sub- or non-performance on the part of the Vendor.

And yet, every SLA must have a starting point. In the course of this review, we have seen two iterations of the SLA draft. The second draft, released just before this review was finalized, represents a significant improvement over the first. It now contains the essential statements of the State's requirements for vendor's data center service performance, as the first draft did not. There remains work to be done on the document to eliminate ambiguities, make language consistent, fill in missing items, and test response time frames. Nonetheless, **we now conclude that the State has the internal resources to identify and state its needs in SLA format.** Of the Project Team members, Data Center Mainframe Operations Director Joe Ng has the greatest direct experience and professional knowledge in data center operations, infrastructure, and trends, and he has taken on a lead or major role in SLA development, with Project Manager Martha Haley coordinating.

We will continue to identify a low impact risk in that the language in the current draft of the SLA has minor shortcomings, as described above. We fully expect these will be resolved as the draft continues to be reviewed and revised. It is important to understand that the SLA is also a legal contract with the vendor. Therefore, we recommend that *legal* expertise be brought to bear on the final iterations, to protect the State as fully as possible.

General Acceptance/Readiness of Staff

See *Readiness to Participate*, above.

Summary

The Project Management Plan (Implementation Plan) includes ample resources, both in timeframe and personnel, to accomplish the Project successfully. We note the necessity of coordinating the various sub-projects, and the need to ensure that the Service Level Agreement being drafted between State and vendor will fully protect the State's interests.

Cost Benefit Analysis

Costs

see Appendix 1, and narrative discussion below.

Benefits

see Appendix 1, Appendix 4, and narrative discussion below.

Narrative Discussion of the Analysis

Benefits to the State

This project represents a net improvement to State data infrastructure; it is not implemented as a cost savings plan. However, project costs are contained within existing operational budget. State employees operating, monitoring, or otherwise managing equipment that will be moved will continue to operate equipment after the move. No State employees are anticipated to be moved as a result of this project (i.e., equipment will be operated remotely, as largely happens now). Any needed personnel for operating the data center facility *per se* (as opposed to the State's equipment hosted within it) are provided by vendor Tech Vault and included in monthly charges. We estimate the 5-year cost of this project at **$3,450,000.00**.

While the costs of this Project are contained within the existing operational budget, the benefits of this project, while intangible, are potentially very large. That is because this Project may be viewed as "insurance" against the risk of data loss or compromise. The existing State data centers replaced or moved in this project, taken as a whole, are quite below industry standards for security, reliability, and recoverability. Recent data center losses during hurricane Irene, while ultimately largely contained, came very close to be catastrophic. If data related, for example, to health care or other State services were permanently lost or compromised, the result would be very difficult. Even a single incident could have very expensive repercussions. The present Project greatly reduces the risk of such loss.

Costs Recovered

The spreadsheet following shows an estimate of costs recovered by pursuing the present project. Three major cost recoveries are paramount: (1) The current cost of the Level 3 colocation facility, which would be retired; (2) Foregoing upgrades to the Cherry St. facility, which would be necessary simply to continue use of the facility; and, (3) Costs recovered by retiring the Barre (McFarland) facility, listed collectively in the spreadsheet as "rent" foregone. The Barre Facility will remain in use for some time after the move to the Tech Vault facility, but would be completely retired by the end of 2013. The rent foregone reflects this short-term continued use. (Note that the scenario of continuing current use of facilities is a very risky approach for data safety, as described above.) We estimate costs recovered over a 5-year period as approximately **$644,111.00**.

COSTS AVOIDED: COMPARISONS TO ALTERNATIVE SCENARIOS

COMPARISON #1: PURPOSE-BUILT DATA CENTER

Taking a somewhat different view, this Project might be compared to an alternative Project of building a new State data center, wholly owned. Building new data centers to state-of-the-art specifications would entail considerable expense. (A new primary data center might cost $8-$10 million.) While the State could decide to pursue this route – for example, by means of a bond issue – the drawback is that the current estimate expects the need for capacity to *diminish* after the initial expansion phase. The State could, therefore, find itself in possession of excess capacity, both in terms of physical space and supporting staff employment, perhaps in a 6-12 year time span. When the capacity was no longer needed, it would have to be discarded or re-purposed, perhaps while the bond issue was still being paid back. The present Project has costs in the range of one-half million dollars per year *already available in operational funds* and could be terminated in a relatively short span of time. The course chosen seems wholly reasonable.

Identifying cost savings in this project therefore depend on answering the question, “Compared to what?” We believe the greatest costs avoided by this project attach to the possibility of data loss or compromise. However, such *potential* losses are impossible to monetize without a study of data contained in the existing centers, identification of risks to those centers, and a review of Disaster Recovery plans, tests, and test results. Even then, only the direct cost to government is identified, not the perhaps far greater cost to the residents of the State, relying on data for business, health care, and services.

However, assuming that the State, through the I-TOP planning process, has decided *not* to do nothing about the existing data centers, we can do a rough comparison to the alternative of building a purpose-built data center owned and staffed by the State. This comparison may be found in Appendix 1 -- Project Costs Details.

We made the following assumptions:

- 3000 sq ft Tier IV data center at $1500/sq ft with 100% margin for Act 250, utility build-out, delays, etc. (Estimate from *datacenterjournal.com*, citing *Data Center Design and Infrastructure Estimates*, an Anixter White Paper.)
- Building depreciated over 39 yrs., straight-line depreciation

- Add'l staffing: 2 technicians, 3 shifts (6 FTE); National avg. salary NOC technician at $44,000.00

Our analysis shows that using a hosted data center is far less expensive for the State. Most of the costs of the hosted center, aside from the actual rack charges, carry to the purpose-built scenario. In addition, significant construction and staffing costs are added. We estimate the 5-year cost of a purpose-built data center to be approximately **$13,978,050.00**.

Comparison #2: Upgrade One Data Center to Industry Standards

In lieu of building a new data center from the ground up, the State could decide to upgrade one of the existing data centers to current industry standards, or at least as close of siting, architecture and facilities would allow. Estimating costs for such renovation is more difficult than in the first comparison, as there exists no "one size fits all" estimating tool that can take into account all the possible idiosyncrasies of existing sites. However, using the document prepared for the State in 2011, Data Center Assessment and Plan, by Electronic Environments Corporation, as a starting point, the most significant needed renovations have been identified and costs estimated. The scenario envisions upgrading one of the two data centers (Barre /McFarland) while retiring the other (Cherry St.). It is estimated that the Cherry St. facility cannot reasonably be upgraded to anything approaching industry standards, because of inherent structural limitations. Additionally, centralizing to a single data center would simplify monitoring, maintenance, and equipment planning, as well as the associated costs.

This scenario is shown on the spreadsheet as Comparison #2 in Appendix 1 -- Project Costs Details. Although the base construction costs are significantly lower than those for a purpose-built data center, it must be noted that many of the other costs, for moving, net gear, and especially staffing, remain the same. This brings the 5-year cost of upgrading one data center to approximately **$3,971,000.00**. Note that this would not meet all industry standards, but only those allowed by the current architecture, site, and facilities. In comparison, the colocation approach is less expensive, but reaches industry standards. See Appendix 4 – Qualitative Benefits.

Summary

This Project enhances State IT operations by moving several components of current data center operations to more appropriate locations. The hosted data center will increase security, reliability, and recoverability, reducing the State's exposure to significant costs from data loss or compromise. These benefits, both tangible and intangible, are significant. Compared to building a new center from the ground up, this Project's savings are very significant. Compared to upgrading an existing secondary data center, this Project's savings are less, but still significant. In both comparisons (purpose-built or upgrade), the State is potentially left with excess cost and capacity, in comparison to the current Project, should the State’s need for data center space contract, as is anticipated.

APPENDIX 1 – PROJECT COSTS DETAILS

see next page for spreadsheet of 5-year project costs and savings

SOV Hosted Data Center Project

5-year Cost Projections

Project Item	2013-14	2014-15	2015-16	2016-17	2017-18	5 year TOTALS
Network Equipment	$ 475,000.00	--	--	--	--	**$ 475,000.00**
Dark Fiber Circuit	$ 140,000.00	--	--	--	--	**$ 140,000.00**
IBM Move Services	$ 25,000.00	--	--	--	--	**$ 25,000.00**
Move Services	$ 25,000.00	--	--	--	--	**$ 25,000.00**
Move Level 3 Connections	$ 5,000.00	--	--	--	--	**$ 5,000.00**
Co-Location Estimate (Rack + Power)	$ 300,000.00	$ 300,000.00	$ 300,000.00	$ 300,000.00	$ 300,000.00	**$ 1,500,000.00**
Dedicated Circuit	$ 96,000.00	$ 96,000.00	$ 96,000.00	$ 96,000.00	$ 96,000.00	**$ 480,000.00**
Maintenance and EQ replacement	$ 160,000.00	$ 160,000.00	$ 160,000.00	$ 160,000.00	$ 160,000.00	**$ 800,000.00**
Yearly Totals	**$ 1,226,000.00**	**$ 556,000.00**	**$ 556,000.00**	**$ 556,000.00**	**$ 556,000.00**	$ 3,450,000.00
Costs Recovered:						
Retired Level 3 Colocation Facility	$ (40,000.00)	$ (40,000.00)	$ (40,000.00)	$ (40,000.00)	$ (40,000.00)	**$ (200,000.00)**
Cherry St. Upgrade Foregone	$ (350,000.00)	--	--	--	--	**$ (350,000.00)**
McFarland (Barre) rent foregone	$ (17,839.00)	$ (19,068.00)	$ (19,068.00)	$ (19,068.00)	$ (19,068.00)	**$ (94,111.00)**
Total Cost with Savings						**$ (644,111.00)**

For Comparison Purposes

Comparison 1: Purpose-built Data Center

Estimate of Costs

Building construction and fitting(a)	$ 9,000,000.00	--	--	--	--	**$ 9,000,000.00**
Building depreciation(b)	$ 256,410.00	$ 256,410.00	$ 256,410.00	$ 256,410.00	$ 256,410.00	**$ 1,282,050.00**
Staffing for 24X7 DCOC(c)	$ 264,000.00	$ 264,000.00	$ 264,000.00	$ 264,000.00	$ 264,000.00	**$ 1,320,000.00**
Network Equipment	$ 475,000.00	--	--	--	--	**$ 475,000.00**
Dark Fiber Circuit	$ 140,000.00	--	--	--	--	**$ 140,000.00**
Move Services	$ 25,000.00	--	--	--	--	**$ 25,000.00**
Move Services	$ 25,000.00	--	--	--	--	**$ 25,000.00**
Move Level 3 Connections	$ 5,000.00	--	--	--	--	**$ 5,000.00**
Power	$ 85,200.00	$ 85,200.00	$ 85,200.00	$ 85,200.00	$ 85,200.00	**$ 426,000.00**
Dedicated Circuit	$ 96,000.00	$ 96,000.00	$ 96,000.00	$ 96,000.00	$ 96,000.00	**$ 480,000.00**
Maintenance and EQ replacement	$ 160,000.00	$ 160,000.00	$ 160,000.00	$ 160,000.00	$ 160,000.00	**$ 800,000.00**
Yearly Totals	**$ 10,531,610.00**	**$ 861,610.00**	**$ 861,610.00**	**$ 861,610.00**	**$ 861,610.00**	**$ 13,978,050.00**

(a) 3000 sq ft Tier IV data center at $1500/sq ft with 100% margin for Act 250, utility build-out, delays, etc.

(b) 39 yrs., straight-line depreciation

(c) Add'l staffing:

National avg. salary NOC technician	$ 44,000.00
2 technicians, 3 shifts	6
	$ 264,000.00

Comparison 2: Upgrade one (Barre) Data Center

Estimate of Costs

Replace Floor Tiles (400 tiles @ $100)	$ 40,000.00	--	--	--	--	**$ 40,000.00**
Replace UPS	$ 105,000.00	--	--	--	--	**$ 105,000.00**
Replace 2 CRAC Units	$ 130,000.00	--	--	--	--	**$ 130,000.00**
Staffing for 24X7 DCOC(d)	$ 264,000.00	$ 264,000.00	$ 264,000.00	$ 264,000.00	$ 264,000.00	**$ 1,320,000.00**
Network Equipment	$ 475,000.00	--	--	--	--	**$ 475,000.00**
Dark Fiber Circuit	$ 140,000.00	--	--	--	--	**$ 140,000.00**
Move Services	$ 25,000.00	--	--	--	--	**$ 25,000.00**
Move Services	$ 25,000.00	--	--	--	--	**$ 25,000.00**
Move Level 3 Connections	$ 5,000.00	--	--	--	--	**$ 5,000.00**
Power	$ 85,200.00	$ 85,200.00	$ 85,200.00	$ 85,200.00	$ 85,200.00	**$ 426,000.00**
Dedicated Circuit	$ 96,000.00	$ 96,000.00	$ 96,000.00	$ 96,000.00	$ 96,000.00	**$ 480,000.00**
Maintenance and EQ replacement	$ 160,000.00	$ 160,000.00	$ 160,000.00	$ 160,000.00	$ 160,000.00	**$ 800,000.00**
Yearly Totals	**$ 1,550,200.00**	**$ 605,200.00**	**$ 605,200.00**	**$ 605,200.00**	**$ 605,200.00**	**$ 3,971,000.00**

(d) Add'l staffing:	
National avg. salary NOC technician	$ 44,000.00
2 technicians, 3 shifts	6
	$ 264,000.00

APPENDIX 2 - PROJECT PLAN MILESTONES

from <u>SOV Hosted Data Center Abbreviated Project Charter</u>, ver. 2.0, 11/20/2012

Milestone	Date
Complete RFP Process	October 2012 –Done
Complete Cost Model	October 2012
Complete Statement of Work for Independent Review process	November 2012
Identify equipment for move to the Hosted Site	November 2012
Begin contract negotiations with Hosted Data Site provider	November 2012
Business Requirement Gathering for SOV & Hosted Vendor Work	November 2012
Sign-Off by CIO on Independent Review	December 2012
Place Order (Selected Bidder) for Network Equipment (& other needed equipment)	December 2012
Sign-off on all Business Requirements	December 2012
Sign Contract with Hosted Data Center Provider (to include SLA, Requirements & Disaster Recovery Plan)	December 2012
Complete Design Plans (SOV network & Vendor site plans) & Sign-off	Jan/Feb 2013

Milestone	Date
Sign Contract with IBM to support Move (Cherry St and McFarland to the hosted site)	Feb 2013
~~Move from 133 State Street to National Life~~	~~Feb 2013~~
Start Builds (Hosted Site & Network to support)	March 2013
Start Testing (Hosted Site Verification & Network Connectivity Testing)	March 2013
Sign-off on Completion of Builds & Testing	April 2013
Sign-off on Move Plan by Sponsor, Stakeholder, Hosted Site Provider, & IBM (plan includes move preparations, Move Day plan & schedule of events, Contingency Plan, etc.)	April 2013
Complete Move Preparations	April/May 2013
Move (PeopleSoft DR racks from Mcfarland, DR mainframe from McFarland, misc. 2 racks from McFarland, and 2 racks from Cherry St), Install & Verify Success - Hosted Site up & Running!	May 2013
Implement Post Live Support Plans (e.g. SLA, SOV Change Management Plan, SOV Roles & Responsibilities, etc.) and Decommission Data Centers (Cherry St. & McFarland)	May 2013
End of Project	May 2013

APPENDIX 3 – RISK MANAGEMENT PLAN

Risk Table Item	Explanation
Risk #	Integer identifying the risk in this document
Risk Area	A general term identifying the general area of project planning where this risk is evaluated. Some likely terms are **PROJECT MANAGEMENT, PROJECT DEVELOPMENT, VENDOR EVALUATION**
Risk Impact	This term indicates our assessment of the severity of damage, should the risk be realized. This term DOES NOT take into account agreed-upon risk mitigation or avoidance plans. Ranking terms are: **[LOW-MED-HIGH]**
Risk Prob[ability]	This term indicates our assessment of the likelihood of risk realization. This term DOES take into account agreed-upon risk mitigation or avoidance plans. Ranking terms are: **[LOW-MED-HIGH]**
Response Time	This term indicates the time frame in which risk mitigation or avoidance should be employed. Terms are: **[PRE-K (i.e., pre-contract) – ONGOING – POST-K (i.e., post-contract)]**
Risk and Description	The risk is named and explained.
Result of Risk Realization	Defines the damage to the State resulting if the risk is realized.
Comment and Recommendation	Further information about the risk and the context, and our recommendation for mitigation.
Mitigation Plan	Mitigation Plan as agreed upon between reviewer and Sponsor (in this case, Sponsor represented by Project Manager, with other participants consulted if appropriate). Mitigation participants are identified by **name and title** (or function, if appropriate).

Risk #: 1	Area: VENDOR EVALUATION Risk Level: HIGH / Risk Prob: LOW Response Time: PRE-K
Risk and Description	**Vendor will not release detailed financials** The State prefers vendors to disclose financial details of their business operations, in order to evaluate the financial stability of the vendor. Tech Vault declined to reveal such details (as a close corporation). They did, however, point to a 25% ownership stake by ICV, as some evidence of financial resources. An example of a question that might be difficult to answer without adequate financial data: Would the vendor be able to continue complete service to the State in the event that vendor loses a large current customer?
Result of Risk Realization	If vendor is not adequately funded, it could fail to perform adequately, or fail completely, even if highly motivated.
Comment and Recommendation	We are told that it is increasingly common for close corporations and privately held companies to decline to release financials when negotiating with the State. The State reserves the right to be flexible in its RFP/RFQ response evaluations and may decide to select a vendor without this data. At the same time, it is likely that this project team has been focused more on the technical performance of the vendor than on financial stability. We recommend that some time be set aside to focus on this issue in collaboration with the appropriate State legal and financial resource persons.
Mitigation Plan	Project Manager Martha Haley will work with Contracts and Procurements Specialist Peter Kipp to ensure that the appropriate State legal and financial expertise is directed to assess this issue. Further communication with Tech Vault on this issue may help in revealing additional supporting evidence of vendor’s financial stability.

Risk #: 2	Area: VENDOR STABILITY Risk Level: MED / Risk Prob: LOW Response Time: PRE-K
Risk and Description	**Vendor's corporate structure may be somewhat unusual** Tech Vault is organized as a Sub Chapter S corporation (Vermont), a structure usually associated with smaller business concerns. This may be somewhat unusual if the State commonly deals with large corporations organized as Sub Chapter C corporations, and/or publicly held corporations. Tech Vault has no employees. The facility is operated and managed by the employees of Tech Group, Inc., an affiliated corporation with a common ownership to that of Tech Vault.
Result of Risk Realization	The State must be able to seek appropriate remedies in the event of injury.
Comment and Recommendation	We are not stating that there is anything wrong or inappropriate about Vendor's corporate structure. We are not making a legal statement, but only noting that this structure (S corp, with all employees from an affiliate) *may* be unusual for the State to encounter in a large contract. We recommend that the State's legal and financial experts satisfy themselves that this structure does not expose the State to undue risk in the event of sub-par performance.
Mitigation Plan	Project Manager Martha Haley will work with Contracts and Procurements Specialist Peter Kipp to ensure that the appropriate State expertise is directed to assess this issue.

Risk #: 3	Area: PROJ MANAGEMENT Risk Level: LOW / Risk Prob: LOW Response Time: ONGOING
Risk and Description	**Project requires timing issues among multiple sub-projects, vendors, supervisors** While this project focuses on the selection of Tech Vault as the vendor for the data center colocation facility, it also encompasses several sub-projects, such as • Moving of mainframe facility (by IBM) • Planning network expansion and build-out of fiber • Acquisition of network gear / building and preparation of new racks In order for the project to go smoothly, the sub-projects must be completed by the designated "move days." This could be difficult as several vendors will be involved, and several individuals will supervise the sub-projects
Result of Risk Realization	If one or more sub-projects are not ready by "move day," the date might be postponed. The State might incur some concurrent costs for overlapping services, negotiated and/or communicated "windows of opportunity" could be missed, causing distress for some State employees or the general public (i.e., those who access AHS web sites).
Comment and Recommendation	The State has chosen to deal with this issue by adopting a sufficiently long lead time for the sub-projects to mature. Since there is little risk in the projects coming to completion too *soon* (with the possible exception of "turning on" Internet connectivity before it is needed). This should be an adequate response. However, it is important that communication throughout the project team about the status of sub-projects *and any change in their respective time frames* continues throughout.
Mitigation Plan	Project Manager Martha Haley, Chief Technology Officer Michael Morey, and Data Center Mainframe Operations Director Joe Ng will strive to maintain a high level of communication concerning the status of sub-projects and their respective relationships to overall project timing.

Risk #: 4	Area: PROJ MANAGEMENT	Risk Level: HIGH / Risk Prob: LOW	Response Time: ONGOING
Risk and Description	**Data and/or equipment could be lost in transition on move day**. The moving of equipment on the "move day(s)" will involve physically disconnecting, carrying across town, reconnecting, and restarting equipment, some of which carries production data. During this sequence, there is probably a greatly increased risk that some misfortune may damage one or more servers, or the data contained therein. The Project Management Plan already includes a path to a contingency plan, but has not yet reached the point of realization.		
Result of Risk Realization	Temporarily lost data and/or down equipment would create delays impacting State employees and, to some extent, members of the public who access AHS web sites. Permanently lost data could incur additional costs.		
Comment and Recommendation	As long as recovery and restoration procedures exist, backups are current, and the equipment is known to be replaceable, any data loss should be temporary. Therefore, we recommend that the Contingency Plan, as it is developed, will include identification and review of these procedures for all moved servers, and creation of such procedures wherever they do not already exist. Any technicians involved in the move should have access to these procedures readily available. We understand that • Many servers are already virtualized, simplifying the recovery plan(s) • There is one DEC Alpha server (Cherry St.) which may not be easily replaceable, because of its age. There should be some plan for what to do if this server is damaged in the move. • The mainframe equipment will be moved by IBM and the above issues are assumed to be addressed for the mainframe		
Mitigation Plan	• Project Manager Martha Haley will oversee the development of a move day Contingency Plan under the Project Management Plan • Project Manager Martha Haley, Chief Technology Officer Michael Morey, and AHS IT Directory Steve Bentley will ensure that team members and their staffs identify and review recovery, restoration, and replacement procedures for all servers to be moved • A contingency sub-plan will be created for any server that cannot be recovered/restored • The Contingency Plan will include a communication plan for any users that may be affected by delay or outage		

Risk #: 5	Area: PROJ DEVELOPMENT Risk Level: MED / Risk Prob: LOW Response Time: ONGOING
Risk and Description	**State personnel could obviate security standards if not properly trained**. While we agree that Tech Vault appears to be a state-of-the-art facility in security terms, we also note that the facility does not have security personnel continuously on site. We believe it is important for the State to recognize the nature of physical security at an unpopulated site, and to enhance training of State personnel to avoid any compromise of strict security protocols, such as bringing unauthorized guests into the facility (which admittedly may be difficult but not impossible) through techniques such as "tailgating" (bringing or allowing a second person into a facility through a secure entrance on the credentials of the first).
Result of Risk Realization	Defeat of high security standards as established by SSAE-16 (etc.) audit(s); in a worst-case-scenario, entry of a dangerous and/or destructive person through the naiveté of a State employee.
Comment and Recommendation	SSAE-16 states that "Data Center Security Staff] "should perform a host of duties on a daily basis, such as monitor intrusion security alarm systems; dispatch mobile security officers to emergencies; monitoring to prevent unauthorized access, such as tailgating; assist all individuals who have authorized access to enter the data center; controlling access to the data center by confirming identity; issue and retrieve access badges; respond to telephone and radio communications." Furthermore, "Any individual requesting access to the data center should be enrolled in a structured and documented provisioning process for ensuring the integrity of the person entering the facility." To maintain physical security at this hosted data center site, State personnel should meet the same standards as those to which the center is audited. This would include the above provisioning process, which presumably would include training to prohibit "tailgating." Development and implementation of such a process would mitigate the risk of lessened security at a site which does not necessarily have data center / security personnel on duty at all times. Additionally, supervisory personnel should adopt a stronger policy of restricting and monitoring data center access.
Mitigation Plan	Joe Ng , Data Center Mainframe Operations Director, will be responsible for designing security protocols on the State side. We note with approval that he has stated: "Access to SOV Data Center at Tech Vault will be more restrictive, since there will be very limited # of people who will have access to this facility. In addition, there will be 2 form of authentication (Card key and access code) for gaining access. This facility should enable us to improve access control. We will also maintain sign-in sheets (IRS regulation) in our facility for people who are authorized but do not have access badge, such as vendor performing maintenance. We plan to escort anyone who is not authorized to access the data center alone. Currently, there is no formal security training. However, with the new security implementation at Tech Vault, we expect new security training is needed for this facility."

Risk #: 6	Area: PROJ DEVELOPMENT Risk Level: LOW / Risk Prob: LOW Response Time: PRE-K
Risk and Description	**Service Level Agreement needs legal review** Developing an appropriate Service Level Agreement (SLA) in the process of negotiating a contract with Tech Vault will be critical to ensuring that the State receives the services it needs and that appropriate remedies are made available for non- or sub-performance. The second draft of the SLA, released just before this review was finalized, represents a significant improvement over the first. It now contains the essential statements of the State's requirements for vendor's data center service performance, as the first draft did not. There remains work to be done on the document to eliminate ambiguities, make language consistent, fill in missing items, and test response time frames.
Result of Risk Realization	Contract negotiations could be delayed if development of an SLA is inappropriately slow. In a *worst case scenario*, the result could be an incomplete and inadequate SLA that puts the State at risk for downtime, data loss, additional expense, or legal action in the event of sub- or non-performance on the part of the Vendor.
Comment and Recommendation	Of the Project Team members, Data Center Mainframe Operations Director Joe Ng has the greatest direct experience and professional knowledge in data center operations, infrastructure, and trends, and he has taken on a lead or major role in SLA development. We will continue to identify a low impact risk in that the language in the current draft of the SLA has minor shortcomings, as described above. We fully expect these will be resolved as the draft continues to be reviewed and revised. It is important to understand that the SLA is also a legal contract with the vendor. Therefore, we recommend that legal expertise be brought to bear on the final iterations, to protect the State as fully as possible.
Mitigation Plan	Data Center Mainframe Operations Director Joe Ng will work with Project Manager Martha Haley to steward the SLA process, and to ensure that appropriate legal review of the Service Level Agreement takes place before contract execution.

APPENDIX 4 – QUALITATIVE BENEFITS

The Tech Vault data center facility represents a significant upgrade from the existing State secondary data centers. The following Executive Summary lists improvements the State gains in terms of industry standards.

Executive Summary

Tech Vault was designed as a data center. The facility structure was built to Homeland Security standards and has achieved LEED Silver certification. It incorporates full redundancy (N+1) for all critical systems. It uses NOVES-1230 Sapphire zero-residual clean agent fire suppression system. HIPPA, PCI, DSS and SSAE-16 (in progress) compliance. It offers improved 2-form authentication access security with a secure area dedicated to the State use only. It provides better infrastructure equipment management and maintenance. It is managed by people who understand the needs and unique challenges of operating a data center.

Facility	• Improved Building construction – Homeland Security standards • LEED Silver Certification
Security	• Improved access control with 2-form authentication • Secured mantrap access • Video surveillance • Dedicated secure area for State use only.
Infrastructure	• N+1 redundancy • Improved power, backup and cooling • NOVEC-1230 Sapphire zero-residual clean agent fire suppression system
Management	• Improved data center management equipment, software, policy and procedures • Managed by people who understand the needs and unique challenges of operating a data center
Compliance	• HIPAA. PCI, DSS and soon to be SSAE-16