



North Carolina
Criminal Justice Law Enforcement
Automated Data Services
(CJLEADS)

Management and Hosting Report
October 2011

North Carolina
Office of the State Controller

David McCoy, State Controller

Table of Contents

I. Executive Summary	2
II. CJLEADS Management	4
A. Accomplishments	4
B. Challenges	6
C. Approach	6
D. Recommendation For Long-Term CJLEADS Management	7
III. CJLEADS Hosting Strategy	11
A. State-Hosted Alternative	12
B. SAS-Hosted Alternative	13
C. Cost Comparison	14
D. Recommendation	17
APPENDIX A	18

I. Executive Summary

Since 2008, the Office of the State Controller (OSC) has managed the Criminal Justice Law Enforcement Automated Data Services (CJLEADS) data integration project in accordance with the direction set forth by the N.C. General Assembly and in close collaboration with its partner agencies including the Administrative Office of the Courts, Department of Correction, Department of Crime Control and Public Safety, Department of Justice/State Bureau of Investigation, Department of Juvenile Justice and Delinquency Prevention, Division of Motor Vehicles, North Carolina Association of Chiefs of Police, North Carolina Sheriff's Association and the Wake County courts.

The initial legislation directed the OSC to create a tool to serve law enforcement and the courts by integrating and providing up-to-date criminal information through a single, secure, web-based application. To accomplish this task, the State Controller selected SAS as a vendor partner and worked with state, local and federal criminal justice organizations to develop and implement the CJLEADS Pilot Program in Wake County.

Consistent with the Legislature's intent to serve criminal justice professionals and improve the safety of North Carolina's citizens, CJLEADS has two primary objectives:

1. To provide a comprehensive view of an offender through a single application, allowing for a positive identification of an offender through a photographic image.
2. To provide an "offender watch" capability to alert criminal justice professionals when an offender has a change in status.

After consolidating more than 42 million records representing 13.6 million offenders and completing a successful Wake County Pilot, OSC initiated a three-phase statewide deployment. Please see [Appendix A](#) for a map of the CJLEADS phased deployment.

OSC began the statewide Phase I deployment in December 2010 to the Upper and Lower Piedmont. Primary activities for the Phase I deployment were completed in June, 2011, by offering all organizations in the Piedmont regions the opportunity to use CJLEADS. To date, 117 local, state, and federal agencies (out of 151 identified organizations) in the Piedmont regions have worked with OSC to gain access to CJLEADS.

The Phase II deployment began in May 2011 to the lower western and lower eastern regions of the State. By June, 2011, Phase II kick off meetings were complete and training in these areas began in July. To date, 119 local, state, and federal agencies in these regions have completed or are in the process of on-boarding their agencies with CJLEADS.

In response to the increasing interest for CJLEADS in the remaining areas of the State, OSC accelerated the schedule for Phase III deployment from December to August and completed kick-off meetings in the upper western and upper eastern regions of the State in September, 2011. To date, 83 Phase III agencies are in the process of on-boarding with CJLEADS.

In total, OSC has conducted 53 kick off meetings with more than 1,200 criminal justice professionals in attendance. Since January 1, 2011, more than 10,000 individuals have been trained and are actively using access CJLEADS.

The response from criminal justice organizations has been extremely positive. Law enforcement officials routinely share success stories with OSC about how CJLEADS has helped them catch and track criminals because of the consolidated data and ease of use of the application.

While the CJLEADS project has achieved a great measure of success, significant work remains. During the next year, OSC will continue to provide CJLEADS training to criminal justice professionals throughout the State. In addition, OSC will continue to develop vital interfaces and functionality, such as federal files, deemed essential to providing a full-service application to meet the needs of criminal justice professionals and fulfill the original mission of the project as outlined by the legislature.

This report fulfills the requirements of Session Law 2011 – 145, HB 200 which directs the OSC to:

- Review plans to transition CJLEADS to the Department of Justice, determining if that is still the best course of action, and identifying an alternative if necessary.
- Provide a recommendation to the Joint Legislative Oversight Committee on Information Technology on the best alternative for managing and hosting CJLEADS, along with a timeline for the transition.

II. CJLEADS Management

Since the inception of the CJLEADS program in October, 2008, OSC has managed the design, development, testing, implementation, deployment and support of the application. The OSC has worked collaboratively with state, local and federal criminal justice organizations to understand the critical business needs of the courts, correction, and law enforcement personnel. Using this information, OSC has leveraged the relationship with SAS and its expertise in data integration, business analytics and reporting to develop a robust, user-friendly system that brings valuable information to criminal justice professionals through a single, secure, and easy-to-use application allowing them to be more efficient and effective in their day-to-day work activities.

A. Accomplishments

OSC, SAS and all criminal justice partner agencies have worked tirelessly to bring CJLEADS through the development process and successfully deploy the application throughout the State. Significant work has been accomplished since October 2008 including:

- OSC and SAS developed a strong working partnership built upon active and engaged executive leadership from both organizations. Executive leadership provided guidance and removed obstacles allowing the project team to focus on design and development priorities. The OSC and SAS teams developed a project management approach that was flexible, collaborative, and guided by regular and open communications. This allowed the team to quickly address development challenges and maintain strong forward momentum with project activities.
- OSC assembled a diverse project team made up of over 100 members representing eight different State agencies as well as Wake County courts and local and federal law enforcement agencies. This team worked together to develop business requirements, define and develop data interfaces and test the system to ensure that the application met the needs of the varied user community.
- The State and SAS project teams developed a robust, reliable technical architecture and end-user application that supports all criminal justice professionals in North Carolina, including court personnel, corrections officers, and law enforcement at the state, local and federal levels. The application contains over 42 million offender information records as well as a real-time interface with DMV for driver license and vehicle registration information. The application offers practical, easy-to-use functionality that enables criminal justice professionals to obtain critical data in seconds, improving the decision making process that helps improve the safety of the public and law enforcement officers.
- OSC deployed the initial release of CJLEADS as the Wake County pilot program in June, 2010. To manage the Wake County pilot, OSC established a business operations team to support user administration, training, and customer support. The Wake County pilot involved deployment of the application to 47 organizations with over 2,500 users trained. In December, 2010, a survey of the Wake County user

community revealed that 99% of respondents found CJLEADS to be of value to their organizations. Ninety-seven percent of respondents indicated CJLEADS made them more effective and efficient in their day-to-day work activities.

- In December, 2010, OSC began the statewide deployment of CJLEADS with Phase I, including the upper and lower Piedmont regions of the State. By June, 2011, deployment kick off meetings for Phase II were complete in the southwestern and southeastern regions of the State, and in September, 2011, OSC completed the kick-off meetings for Phase III, the northwestern and northeastern regions of the State. Due to the increased demand for CJLEADS, the schedule for Phase III was accelerated, and the deployment process is three months ahead of schedule. To date, over 359 organizations have signed on to use CJLEADS, and we have trained over 10,000 end users.
- While the statewide deployment has been on-going, OSC has continued to design and develop mission critical data and functionality for the CJLEADS application as outlined in the original legislation establishing CJLEADS. Design and development has followed an iterative, phased approach allowing the application to be developed module by module. As each module is completed and tested, new releases of the application are issued, making new data and functionality available to existing users. The following releases have been successfully deployed:
 - Release I (June, 2010) - Administrative Office of the Courts court records and un-served processes, Department of Corrections incarceration and probation/parole information, jail booking information, and offender watchlist and auditing functionality.
 - Release II (December, 2010) – Department of Justice NC Sex Offender Registry data and a real-time interface with Division of Motor Vehicles driver license and vehicle registration data, night vision, and reporting.
 - Release III (June, 2011) – Department of Justice Concealed Handgun Permit information, user activity access and reporting, application refinements.
- All of the highlighted achievements have been accomplished during challenging economic and budgetary conditions. To date approximately \$17.65 million has been spent on CJLEADS development and deployment. The estimated expenditures for FY 2011 – 2012 will be \$7.7 million for a total development and deployment cost of \$25.3 million. With great attention to costs, OSC management has taken action whenever possible to reduce costs including delaying staff hiring to support and deploy the application, working closely with State agencies, local law enforcement and community colleges to use free or low-cost training facilities to minimize training costs, and collaborating with the Department of Justice to leverage existing 24x7 customer support services rather than establishing a separate help desk staff. These efforts have allowed the project to be completed slightly under the original cost estimate of \$27 million.

While the CJLEADS team has accomplished a great deal, there is still considerable effort required to fulfill the mission set forth by the General Assembly. Work is continuing for Release IV and V of the application with effort focused on wildlife hunting, fishing

license and vessel registration information, federal “Hot Files,” as well as DMV partial plate searches, facial recognition capability, and offender merge options.

B. Challenges

Data sharing requires agencies to embrace a new collaborative approach to provide the information needed to support criminal justice professionals statewide. OSC faced a number of challenges in bringing this enterprise data sharing and integration initiative to fruition:

- Agencies initially demonstrated a strong sense of protectionism toward their data. Significant time and effort was focused on building trust and establishing protocols and procedures that ensured data was accurately received and integrated into the system.
- The majority of criminal information is a matter of public record. Some data, however, is considered sensitive and confidential information including the court’s un-served processes, social security numbers, and the Federal Bureau of Investigation (FBI) number. To ensure that information was readily available to all criminal justice professionals while maintaining required security measures and restrictions for confidential information, stringent role-based security was developed to manage access to data and functionality.
- Requirements for local jail data that is collected by a third-party contracted entity presented legal and contractual issues that required resolution before the information could be integrated. OSC, under the guidance of legal counsel, executed contracts and memoranda of understanding as necessary to secure the data.
- Special clearance was required for OSC and SAS project team members who were not criminal justice professionals. All team members requiring access to criminal data to develop application functionality as well as test and support the system are cleared through an SBI criminal background check and are required to sign a non-disclosure agreement. SAS employees with direct access to the criminal justice data or technical infrastructure are required to review Criminal Justice Information System (CJIS) security policy and agree to follow the policy by signing a CJIS Addendum certification document.

C. Approach

OSC, along with SAS and agency partners, has worked to meet the mission set forth by the General Assembly, achieving great success by dealing effectively with the challenges presented by this complex data sharing initiative.

- OSC acknowledged early in the project the lack of criminal justice experience among its members. Therefore, OSC quickly assembled agency representatives and subject matter experts with various criminal justice backgrounds. As a result, OSC became an objective third-party agency that could listen to and understand the business requirements from a variety of perspectives, including the needs of court personnel which can differ from those of corrections or juvenile justice personnel and are different still from law enforcement. Working closely with the representatives from

each of these user communities, OSC set priorities, made design decisions and directed resources to maximize the results for the user.

- The General Assembly mandate clearly directed OSC to facilitate the involvement and support of the data agency partners. When OSC was faced with challenges during the course of design and development, the legislation provided the foundation for all activities and the encouragement to partner agencies to come to the table and share information necessary to meet the needs of criminal justice professionals.
- A strong communication plan ensured that the CJLEADS efforts were publicly promoted wherever and whenever possible. Quarterly status reports to the legislature, monthly meetings with the State team members, presentations at seminars and conferences for groups such as the NC Conference of District Attorneys, Law Enforcement Planners Association, as well as individual meetings with legislators and the leadership of partner agencies, allowed OSC to share the CJLEADS mission and provide transparency in all actions and decisions. In addition, information regarding various milestones and kick-off meetings were routinely sent to media outlets throughout the State.
- As early OSC communications began to spread the word concerning the CJLEADS mission, grassroots awareness began to develop and many end-user organizations began to offer support, suggestions and feedback on the system.

D. Recommendation For Long-Term CJLEADS Management

While the OSC currently manages the CJLEADS application, the Legislature has requested a recommendation for the long-term management of CJLEADS.

Data integration applications are unique from typical information systems. By design they integrate information across disparate data sources and cross lines of business. CJLEADS, for example, integrates data from a variety of source systems and supports users who serve in different roles throughout the criminal justice community. The challenge, therefore, is to manage data integration systems such as CJLEADS in a manner that:

- Promotes open and consistent data sharing.
- Understands the strategic vision and business needs of participating organizations, and sets priorities for application development and support accordingly.
- Ensures the State's investment is properly maintained and enhanced to provide vital, up-to-date tools to meet end user needs.

To make a recommendation for CJLEADS long-term management, OSC must consider the long-term strategy for current and future data sharing initiatives. As other data integration efforts evolve, each initiative will present opportunities to share valuable information compiled for previous projects to meet new business needs. The ability to leverage the integrated offender information, for example, for future initiatives such as fraud detection is a key component of the overall data integration strategy.

In addition, the management recommendation must consider the strategic vision for criminal justice initiatives and the need to protect the State's investment in CJLEADS

through active maintenance and enhancement to ensure the application remains up-to-date from a technology and business perspective.

There are two feasible alternatives regarding management of the CJLEADS program: 1) retain management of CJLEADS under the OSC Data Integration Program, or 2) transition the management and support of CJLEADS to a criminal justice agency. With either approach, it is imperative that strategic direction continue to support the sharing of the State's data resources for enterprise initiatives and that application support focuses on continuous improvement for new and changing business and technology needs.

Option 1: Retain the Management of CJLEADS Under the OSC Data Integration Program

The OSC Data Integration Program has a proven record of success. It has demonstrated the ability to communicate effectively with a variety of state, local and federal agencies, to interact with all levels of an organization, and to understand business needs and develop solutions that meet and often exceed the expectations of the users. As OSC is charged with the development of other enterprise data integration efforts, such as the fraud, waste and improper payments detection program, continuing to manage CJLEADS centrally would allow all data integration initiatives to use common practices and technology, further improving the delivery and management of data integration programs.

One advantage of this option is OSC's ability to provide a consistent management approach to data sharing, application support, and policies and procedures. Centralized management under the OSC Data Integration Program allows for data integration projects to share a common strategy of leveraging the State's data assets for improved analytics, reporting and decision making.

As an enterprise organization, OSC would objectively guide data sharing and integration efforts in order to integrate data to support multiple enterprise objectives. For example, the offender data that has already been integrated for CJLEADS may provide valuable information to support future initiatives such as the fraud detection program.

Centralized management of multiple data integration applications also will provide the opportunity to share development, infrastructure and support costs. For example, the experience gained with the integration of the North Carolina Identity Management System (NCID) for CJLEADS user authentication will provide a model for future projects, reducing the development time and cost. High-cost hardware components needed for specific technical requirements can potentially be used to support multiple projects achieving greater value by cost sharing across project budgets. Finally, this centralized management approach provides the opportunity to continually update and improve integration applications as new technical capabilities are identified with other data integration projects.

If this centralized management approach is chosen, OSC will work closely with the CJLEADS Leadership Council and partner agencies to ensure that business objectives continue to be met as the application grows and evolves.

A centralized management approach will, over time, result in the OSC Data Integration Program supporting multiple data integration programs. To effectively manage these systems, the program staff must develop and maintain a breadth of knowledge about different business areas, such as criminal justice, fraud and waste, medical claims processing, financial management, and others. To keep systems up to date and to maintain the value of the integrated systems, this central organization must remain actively engaged in the strategic planning and key mission and objectives of these many business units.

Option 2: Transition the Management and Support of CJLEADS to a Criminal Justice Agency

A second alternative for long-term CJLEADS management is to transition CJLEADS to a criminal justice organization. This approach would follow a long-term strategy of decentralized management for data integration applications. Under this scenario, the OSC Data Integration Program would manage the initial design and development of new data integration initiatives, as it did with CJLEADS. Upon completion of the application development, the application would be transitioned to the appropriate business owner for operations support and management.

With this alternative, the CJLEADS operational responsibility and personnel will be transferred to a criminal justice organization as the system nears full deployment and all major development modules are completed. The advantage to this approach is that CJLEADS will be managed by an organization that is responsible for the administration of criminal justice activities and has experience in working with criminal justice professionals throughout the State.

This approach would set a precedent for future data integration initiatives. New data integration projects would remain under OSC management during design, development and implementation and would benefit from the technical expertise and lessons learned from each of the previous data integration projects. Upon the completion of the design and deployment efforts for each project, the application would be transitioned to the business owner, an organization with full business knowledge and understanding. This organization would assume the management and support of the system built to meet the needs of their organization and its users.

The challenge with this approach, both for CJLEADS and future projects, is that data integration projects often serve multiple business areas, data is shared from a variety of sources, and users represent varying roles and responsibilities. As a result, it may be difficult to identify the most appropriate business owner. The managing organization must embrace the strategic vision of the data integration application and strive to encompass the needs of all organizations using the system.

With CJLEADS, management could transition to a law enforcement organization or to a court organization. In either scenario, the CJLEADS business owner must consider the business needs of all project stakeholders. It will be critical for the criminal justice managing organization to understand and share the strategic vision of data integration and to support data sharing of offender information beyond the criminal justice community in support of other initiatives such as fraud detection.

To ensure that all data integration applications continue to focus on supporting the information needs of all enterprise stakeholders, OSC will work with the legislature to require the criminal justice managing organization to periodically report status to the OSC Data Integration Program and to seek guidance in the development of future enhancements. The purpose of this communication is to maintain a consistent approach to managing CJLEADS and other data integration projects throughout the State.

Recommendation

The Strategic Plan for Data Integration sets forth an enterprise approach to data integration. This plan espouses common project management techniques, common technology, common data governance and standards and an enterprise vision for sharing information to support the State's business needs.

CJLEADS has become a robust, broad source of information for criminal justice professionals throughout North Carolina. The State has invested significant time and resources in developing a cutting-edge, integrated system to meet the needs of law enforcement and the courts. To protect the investment the State has made in CJLEADS, it is critical to provide a mechanism to continually enhance and refine the system based on the needs of the criminal justice community and to ensure that the application maintains pace with advances in technology.

While the system currently operates 24x7 in support of criminal justice professionals, the data incorporated into CJLEADS can also provide great value to future data integration initiatives. One example will be the ability to leverage offender information to aid in detecting fraud, waste and improper payments in State government.

Centralized management of CJLEADS, as well as future data integration applications, will allow a project to be managed with an enterprise view of data stewardship and sharing, a focus on technology, and an emphasis on continuous improvement.

Therefore, OSC recommends that the Data Integration Program retain management of the CJLEADS application. OSC will work closely with the business stakeholders, the General Assembly, and the Data Integration Steering Committee to ensure that management direction remains focused on a criminal justice strategic vision and that CJLEADS continues to provide a valuable tool to protect the safety of North Carolina citizens and criminal justice professionals.

III. CJLEADS Hosting Strategy

During the initial stages of the CJLEADS pilot program, the timeline set forth by the General Assembly was very aggressive. To meet this timeline, SAS established a technical data center environment to support CJLEADS. As the project progressed, the technical architecture was fully developed and implemented in the SAS data center. The General Assembly has requested a recommendation for the long-term hosting of the CJLEADS technical infrastructure.

Background

The CJLEADS technical architecture provides for two identical “active-active” production environments. In the normal course of operations, usage of the system is balanced across the two identical environments. During maintenance or technical difficulties in one environment, the users can be directed seamlessly to the second environment while the maintenance is completed or the issue is resolved, allowing for continuous 24x7 hours of operation.

In addition to dual active-production environments, technical environments were established for development and testing of the application. Whenever a new module is developed for CJLEADS, the test, development and production environments are used as the new feature moves from the initial design idea to a fully implemented production module. Each of these technical environments is critical to the development, support and maintenance of CJLEADS.

CJLEADS is an inquiry-only application with an easy-to-use interface for criminal justice professionals. Behind the scenes, however, CJLEADS is a complex technical environment comprised of many different technologies and platforms that allows for disparate data from many sources to be accurately compiled into offender profiles. The system infrastructure has been built, refined, and managed to ensure that the system is robust, available 24x7, and provides the needed performance to support law enforcement personnel in the field.

The support and management of the CJLEADS technical environment is challenging, requiring highly skilled, experienced resources in the areas of data extract, transformation, and load, network, security, database design, web services, and user interface development. SAS has provided data center hosting services, application technical support and application design and development services for nearly three years during the pilot and production stages of the project.

During the initial phases of the project, the plan was to migrate the CJLEADS technical environment to a State-hosted data center facility during the current fiscal year. While the initial contract with SAS provided for the transfer of production hardware and operating software to the State during that transition, the State would be required to purchase additional hardware to support the development and test environments as well as disaster recovery capabilities. In addition, data center infrastructure including telecommunications lines, power supplies, and even floor space were cost considerations in the migration proposal.

For FY 2011-2012, OSC submitted a budget expansion request of approximately \$2.7 million to support the migration of the application to the DOJ data center. The budget expansion funds would have provided for the one-time purchase of hardware, upgrades to data center and communications infrastructure, and SAS services to plan and support the migration activities. In addition, recurring funds were requested to establish and fill technical positions that would manage the migration and support the State-managed application.

Given the economic conditions and budgetary constraints, the budget expansion request was not approved and the migration was delayed indefinitely. This delay will result in a higher cost to migrate the application in the future as the current production hardware in place at SAS will have aged and will need to be refreshed as part of the migration process.

In the interim, OSC negotiated a cost-effective hosting contract with SAS, and they have continued to provide excellent technical support and hosting for CJLEADS.

A. State-Hosted Alternative

Hosting CJLEADS in a State-hosted environment allows the State to maintain complete control over the technical infrastructure and application software and data. With that management control, however, comes the need to provide adequate data center space, technical infrastructure, and highly skilled personnel resources capable of supporting the complex technical environment.

Advantages

Hosting the CJLEADS application allows the State to have complete control over the technical and application environment including:

- Scheduling maintenance and upgrades to hardware.
- Securing the physical infrastructure.
- Managing data interfaces and all data storage.
- Managing all aspects of the application development and support activities.

Disadvantages

The CJLEADS system represents a complex technical and application environment. The challenges to supporting the technical environment include:

- Managing complex hardware components that require specific, highly skilled technical expertise in each area.
- Managing complex software components that require extensive SAS experience.
- Maintaining on-going support contracts with SAS to resolve critical technical issues.
- Maintaining skilled technical staff on the State's payroll which can be challenging given private sector market rates for desirable skill sets.
- Managing and funding hardware refreshes, upgrades and maintenance.

- Coordinating multiple vendor-supported components needed to maintain the CJLEADS environment, including support and services contracts.
- Providing technical and application support for 24x7 operations.
- Funding the cost to migrate the application, estimated to be over \$3 million.

B. SAS-Hosted Alternative

SAS has provided the technical hosting environment for nearly three years, managing all security, operations, and technical support as well as meeting the performance metrics in the service level agreement. SAS acts as a host to a variety of highly secure customer applications and has proven experience in securing and effectively meeting the needs of their customers. Security has been a priority throughout the CJLEADS project. In hosting CJLEADS, SAS has provided clear, documented security policies defining stringent virtual and physical security protocols, conducted regular penetration testing to identify and resolve any vulnerability in the CJLEADS application and technical environment, and participated with OSC and the State Bureau of Investigation in Federal Bureau of Investigation audit activities.

With the indefinite delay of the migration of the application to a State-hosted data center environment, OSC negotiated two additional years of hosting services with SAS to include operational hardware support and maintenance as well as application support.

Advantages

Hosting the CJLEADS application at SAS allows the State to leverage SAS' vast technical resources to provide:

- Highly skilled SAS software support resources to resolve application issues.
- Highly skilled hardware and environment support resources to resolve technical or environment issues.
- Strong SAS partnerships with key technical vendors including database, security, hardware and network to allow for quick resolution to complex issues.
- SAS Research and Development resources to assist the SAS CJLEADS team in resolving issues and evaluating new technologies to improve the application.
- Regular maintenance schedules as well as upgrades and hardware refreshes built into the hosting services contract.
- Technical support resources to manage the 24x7 operations in the SAS data centers.

Disadvantages

The vendor-hosted solution requires detailed negotiations, constant communication and close partnership in the management of the application. Challenges to hosting in a vendor-managed environment include:

- Coordinating system maintenance with SAS schedules and timelines.
- Establishing service level agreements to ensure performance-driven management and support expectations.

- Setting policy and procedures for development, support and issue resolution activities.
- Committing to a long-term hosting agreement as migration to the State is a lengthy and complex process.
- Negotiating reasonable, cost effective hosting services over the long term to avoid unexpected and costly rate increases.

C. Cost Comparison

To provide on-going operations and enhancement, support and deployment, there are various costs to consider when evaluating the State-hosted versus SAS-hosted alternatives.

Some of the cost components associated with CJLEADS operations are the same regardless of the hosted data center environment including:

- SAS software license and usage fees to support the CJLEADS application as well as all criminal justice professionals throughout the State.
- State personnel to support the business design, development, testing and implementation process.
- State personnel to manage the business operations including user administration, training, customer support services and audit activities.
- Basic operations expenses including computers, phones, software licensing, supplies, etc.

Design, development and enhancement funds would also remain the same in either the State or SAS-hosted environment. The design and development funds allow the CJLEADS project team to work with the partner agencies to continue to add mission critical data and functionality to the application, as well as to refine and improve existing functionality. In addition, technology is constantly moving forward and these funds allow the system to remain up to date with changing business needs and emerging technology and avoid the typical scenario where an application remains stagnant for several years and soon becomes obsolete. An example of this ever-changing technology is the current move to mobile computing devices. CJLEADS was architected for desktop and laptop computers. Many organizations are already beginning to move to mobile tablet and smartphone devices. CJLEADS must develop a mobile application version in order to remain current, useful and of value to criminal justice professionals in the field.

While some costs will remain the same regardless of whether CJLEADS is hosted at the State or at SAS, other cost components will vary depending on the hosting decision.

If CJLEADS is hosted at SAS, for example, the State must negotiate a technical hosting contract and an application support contract. The hosting contract provides technical infrastructure, data center space, technical resources, 24x7 support and infrastructure maintenance and upgrades. The application support contract provides technical resources to manage the CJLEADS application including supporting normal production system processing, correcting application issues, monitoring system performance and managing minor application enhancements.

Alternatively, if CJLEADS is hosted at the State, the State must hire a team of technical personnel to support the hardware, network, databases, security and other infrastructure as well as SAS programmers to support the application. Resources must be available to provide 24x7 support for the application and its user community. In addition, following the initial cost of migration, the State must manage the maintenance, upgrade, and refreshes of hardware, network, security, and telecommunications components of the infrastructure.

The final cost component to consider is the expense of the migration of the technical environment from SAS to the State-hosted environment as well as the cost of establishing a geographically diverse disaster recovery environment. The estimated budget expansion request to support the migration will include \$1.7 million in hardware and infrastructure, \$900,000 in migration support services from SAS, and \$735,000 in new State positions for a total estimated migration cost of \$3,335,000. Establishing a geographically diverse disaster recovery environment is estimated to be another \$600,000. State procurement policy allows the cost of the \$1.7 million in hardware and infrastructure for the production/test/development environments and the \$600,000 for the disaster recovery hardware to be spread across four years for budgeting purposes.

The chart of the following page compares the operating expenses between the State-hosted environment and the SAS-hosted environment. With long-term negotiated rates, a SAS-hosted technical environment is slightly less costly than the State-hosted alternative. Maintaining the SAS-hosted environment also provides a cost avoidance of nearly \$3.2 million by not migrating the application to the State and not establishing the geographically diverse State-hosted disaster recovery environment.

Cost Estimates for CJLEADS Hosting Alternatives

	FY 2012	FY 2013 including migration		FY 2014 including DR		FY 2015		FY 2016		FY 2017	
	SAS Hosted	State Hosted	SAS Hosted	State Hosted	SAS Hosted	State Hosted	SAS Hosted	State Hosted	SAS Hosted	State Hosted	SAS Hosted
CJLEADS - Costs Not affected by Hosted Location											
State Personnel/Contract Staff	2,081,377	2,081,377	2,081,377	2,081,377	2,081,377	2,081,377	2,081,377	2,081,377	2,081,377	2,081,377	2,081,377
Operations Costs - (SAVAN, Help Desk, Training, Computers, VPN, Webservers)	246,360	285,000	285,000	285,000	285,000	285,000	285,000	285,000	285,000	285,000	285,000
SAS Licensing	2,000,000	2,000,000	2,000,000	2,000,000	2,000,000	2,000,000	2,000,000	2,000,000	2,000,000	2,000,000	2,000,000
Other Agency Development		150,000	150,000	150,000	150,000	150,000	150,000	150,000	150,000	150,000	150,000
Development/Enhancements	1,324,000	1,200,000	1,200,000	1,200,000	1,200,000	1,200,000	1,200,000	1,200,000	1,200,000	1,200,000	1,200,000
Total CJLEADS Costs Not Affected By Hosting	5,651,737	5,716,377	5,716,377	5,716,377	5,716,377	5,716,377	5,716,377	5,716,377	5,716,377	5,716,377	5,716,377
CJLEADS - Costs Affected By Hosting											
State Personnel for Hosted Technical Support		735,500		735,500		735,500		735,500		735,500	
SAS Hosting Services	1,330,000	700,000	1,500,000		1,500,000		1,500,000		1,500,000		1,500,000
Application Support	724,000	780,000	780,000		800,000		800,000		800,000		800,000
SAS Application Contract Support				800,000		800,000		800,000		800,000	
SAS Customer Care Tech Support				200,000		200,000		200,000		200,000	
Hardware Refresh **											425,000
Communications/Power/VPN/Certs/Enterprise Charges		125,000		125,000		125,000		125,000		125,000	
Other Software Licensing		80,000		200,000		200,000		200,000		200,000	
Total Hosting	2,054,000	2,420,500	2,280,000	2,060,500	2,300,000	2,060,500	2,300,000	2,060,500	2,300,000	2,485,500	2,300,000
CJLEADS Total Cost excluding migration costs	7,705,737	8,136,877	7,996,377	7,776,877	8,016,377	7,776,877	8,016,377	7,776,877	8,016,377	8,201,877	8,016,377
CJLEADS - Migration Costs											
SAS Migration Services		900,000									
Hardware/Infrastructure *		425,000		425,000		425,000		425,000			
DR Environment				150,000		150,000		150,000		150,000	
Total Migration		1,325,000		575,000		575,000		575,000		150,000	
CJLEADS Total Cost	7,705,737	9,461,877	7,996,377	8,351,877	8,016,377	8,351,877	8,016,377	8,351,877	8,016,377	8,351,877	8,016,377

* Hardware estimates are approximately \$1.7 to establish two new active/active production environments and development/test. Based on State procurement, this cost can be spread across four years for budgeting purposes. In FY 2014, hardware to create a geographically diverse Disaster Recovery Site will be needed. This cost can also be spread across four years for budgeting purposes.

** Subsequently, the hardware budget will provide for a 4 year refresh/growth cycle. These estimates are subject to change with technology modifications such as different hardware or database solutions.

D. Recommendation

The OSC has given significant consideration to the CJLEADS hosting recommendation. Based on the successful partnership with SAS during the last several years in hosting and supporting CJLEADS, it is recommended that the State negotiate a long-term agreement to continue operations in the SAS data center environments.

Based on cost analysis outlined above, the cost of hosting in the vendor environment versus hosting in the State environment is comparable on a year-by-year basis, with the SAS solution slightly less than the State-hosted option. The cost of migrating the application at some point in the future and establishing a geographically diverse disaster recovery environment, however, is estimated to be an additional \$4 million.

SAS has demonstrated reliable and consistent management of the CJLEADS infrastructure and application. With CJLEADS hosted at SAS, the State can leverage the broad technical resources available to an organization such as SAS to provide rapid response, cutting-edge technological innovations, and secure and reliable management of its application.

APPENDIX A

CJLEADS Regional Deployment

