

Technology Acquisition Project Case Study

Kansas Criminal Justice Information System

This case study focuses on Internet/Intranet technology acquisitions and related applications. It is one of 18 case studies prepared for the "Technology Acquisition Project" administered by the Institute for Law and Justice in partnership with Government Technology, Inc., and funded by the National Institute of Justice (NIJ), U. S. Department of Justice. The author of this case study is Julie Wartell, Senior Research and Technology Associate, Institute for Law and Justice. The report has been reviewed by the participating site but should be considered a draft pending final NIJ review.

Background on the Project

This case study focused on the acquisition and implementation of Internet/Intranet technology and associated applications within the Kansas criminal justice community. The overall project is a statewide Criminal Justice Information System (CJIS) that allows local and state law enforcement to share data and information through a virtual private network (VPN). The CJIS project is entirely Internet/Intranet-based. There are a number of other systems and applications that run on a separate, statewide network. Although the entire project is touched on in this case study, primary emphasis is on the acquisition process for the Internet/Intranet technology.

Role of the Coordinating Council and Advisory Board

The Kansas Criminal Justice Coordinating Council (CJCC), created by statute in 1994, is leading the effort. The CJCC, assisted by the Criminal Justice Advisory Board (CJAB), has 20 agency representatives from local and state law enforcement, prosecution, courts, defense, corrections, sentencing, the youth authority, information systems, education, and health. The CJAB was used to build a coalition between state and local agencies; the state would have been unable to convince the Legislature without broad-based local support. As vital as the CJAB was to project success, many also credit as important factors the leadership of the Kansas Bureau of Investigation (KBI) and the assistance of Steve Davis of MTG Management Consultants. The key people involved in Kansas CJIS are Carey Brown, CJIS Director; Neil Woerman, Director of Special Projects and Chief of Staff, Office of the Attorney General; Charles Sexson, Assistant Director, KBI; Ken Justice, Kansas Highway Patrol and State NCIC CITO; and Ron Rohrer, Information Resource Manager, KBI.

An immense amount of planning went toward the CJIS effort. A strategic plan was created in April 1996 and updated in July 1997. As described later, the plan includes project background, vision and mission statements, goals, initiatives, plans, a schedule, and a budget.

Report Organization

After briefly summarizing the technology solution, this report discusses technology acquisition as a four-phase process involving (1) assessment and decision making, (2) procurement, (3) implementation, and (4) impact.

Attachment 1 is an organizational chart showing the governance structure for the CJIS, and Attachment 2 shows the CJIS “network.” Attachment 3 is a brief report providing an overview of the Local Application Project, which is integrated with CJIS. A separate case study was also completed on the statewide AFIS (Automated Fingerprint Identification System) that was part of the Kansas CJIS.

Summary of the Technology Solution

The completed CJIS will include the following subsystems:

- Computerized Criminal History System (CCH)—arrests, court dispositions, custody and supervision
- Kansas Incident-Based Reporting System (KIBRS)—law enforcement incident reports
- Automated Fingerprint Identification System (AFIS)
- Automated Statewide Telecommunications and Records Access (ASTRA) Network—central computer, network, and local terminals for law enforcement and criminal justice communication.

The central component of CJIS has a number of servers, including three that are Internet-based: CJIS Web (KBARS), CJIS Mail, and CJIS Public Access. CJIS Web is housed at KBI, while the Mail and Public servers are located at the Department of Information Systems and Communication (DISC). Any web browser offers access to CJIS information. General information includes project status reports and meeting minutes, links to other sites and resources, and bulletin information. In addition, there is online access to some CJIS Central Repository information such as criminal history, hot files (misdemeanor warrants, missing persons, sex offenders, etc.), and KIBRS data. The Public Access server will offer the same accessibility but for a nominal charge. The Mail server is Microsoft Exchange, and all CJIS users who currently do not have email accounts with their agency will have accounts.

A large number of vendors were involved in CJIS. Paradigm4 lead the reengineering of the Central Repository (to include the front end applications of the various subsystems and web server); Business Software & Equipment (BSE) created the local law enforcement interface; and FishNet Security handles security issues using CheckPoint, Entrust Technologies, Internet Security Systems, Security Dynamics, and Netscape systems. The total CJIS budget is \$12 million. The major expenditures were \$2.8 million for AFIS, \$3.6 million for the Central Repository, \$2.5 million for the ASTRA network, \$2 million for local systems; and \$1 million for network security.

Assessment and Decision Making Phase

Problem Statement

Implementation of Sentencing Guidelines in 1994 was a deciding factor for the state to make some long needed changes. There was a need to quickly access complete criminal history information for sentencing purposes, and at the time, it was not readily available. The state admitted to being very behind in the use of technology. The Kansas Legislature created the Criminal Justice Coordinating Council (CJCC) in 1994 to bring together key policy makers from major agencies to oversee the state's criminal justice information systems. The CJCC, with assistance from the Kansas Sentencing Commission (KSC) and the KBI, began with a plan to automate records and eventually saw the need for a much larger, more encompassing criminal justice information system.

In 1995, the KSC audited the state's criminal history repository. The audit showed a large percentage of records not entered, inaccurate, or missing information. As a result, the state contracted with MTG Management Consultants for a needs analysis of the state's information systems and the ASTRA network.¹ The analysis examined the data collection and dissemination processes, the technology environments of several counties, and system shortcomings. In addition, a data dictionary and business function model were developed. The needs analysis found distinct problems relating to governance, policy, forms and procedures, management, data, and technology.²

Records Automation Project

Several federal initiatives also played a role in the initial Records Automation Project and subsequent criminal justice information system. These included the Criminal History Records Improvement Program (1990), Crime Control Act/Edward Byrne Memorial State and Local Law Enforcement Assistance Program (1990), and National Criminal History Improvement Program (1994).

The Records Automation Project, which began in September 1996, was a precursor project but was integrally linked to CJIS. Automating records was the short-term goal that was the basis of the much larger, far-reaching system that the CJCC envisioned.

CJIS Strategic Plan

An elaborate planning process, with participation from a variety of state and local agency personnel, was completed before going forward with CJIS. The outcome was a detailed, thorough Strategic Plan, based on data collection and analysis, strategy development, and implementation planning. The mission of CJIS, which drove the plan's development, is "to create and maintain an accessible, and appropriately secured, criminal justice information repository with accurate, complete, and timely data on individuals and events for criminal justice and non-criminal justice users that supports

¹ MTG eventually served as the consultant for the entire process. Project staff were very satisfied with MTG's assistance and felt they played an important role in overcoming interagency politics, convincing the Legislature of the need for CJIS, and keeping the people involved and the project going.

² See State of Kansas Criminal Justice Information System Strategic Plan, 1997, for a description of the specific problems.

effective administration of the criminal justice system, public and officer safety, and public policy management in a cost-effective manner within the state of Kansas.”

Moreover, the strategic plan has nine goals for CJIS; briefly, these are to

1. Develop and maintain an accurate, comprehensive collection of criminal history information that meets local, state, and federal standards for data quality and timeliness.
2. Ensure compatibility with the emerging national criminal justice information environment.
3. Increase use of the system by providing on-line access to the appropriate information for the system’s primary and secondary customers.
4. Ensure the systems’ ability to migrate over time with technology advancements.
5. Increase cost effectiveness by reducing the manpower associated with system inputs and outputs at both the state and local levels.
6. Ensure the state’s ability to manage and continue to expand the system’s functionality.
7. Increase public safety by developing and implementing a centralized criminal justice information repository.
8. Provide operational, statistical, and policy data seamlessly to all authorized members of the criminal justice community.
9. Maintain a CJIS that respects the privacy rights of every citizen in Kansas.

The above goals are being accomplished through ten strategic initiatives, each of which involves several projects.

Project staff felt this strategic planning process was important to promote the CJIS concept and to gain credibility and buy-in for a state project.

Data Accessibility and Management Needs

Prior to 1998, accessibility to statewide information was still extremely limited. The network connection was slow, and only text-based data could be downloaded; law enforcement outside of Topeka could not see fingerprints or photos stored at KBI. In addition, the present transmission protocol, through Tandem Computer switches, was not Y2K compliant. The CJCC and project staff wanted a new system that would “fix” all of the existing automation and data management and dissemination issues. In addition, they wanted this system to use the Internet; be secure; provide timely and accurate data; be paperless; provide fast, low cost communications (via email); be personal computer-based; and use Microsoft solutions (NT, SQL, VB, Exchange, and Office).

Options Considered

One option discussed was to develop a private network. This would have cost \$2.5 million a year more than the virtual private network (VPN) (a cost shared between KBI and local law enforcement) and would have entailed purchasing hardware, doing installations throughout the state, and managing the network. Another option was to use the existing Kansas Wide Area Information Network (KANWIN). KANWIN is a frame relay backbone that supports TCP/IP, Novell Internet Exchange Protocol, and SNA. Security was extremely important in the decision to develop a VPN. The primary reasons for top-notch security were the use of an open system architecture, the need to share electronic data using public Internet service providers, and FBI requirements. Proper security meant protecting data and machines on the KBI LAN as well as transmissions over the Internet. In addition, they wanted to be able to identify the user and the machine being used, monitor for unauthorized intrusion, and analyze network vulnerability.

Project Organization and Staffing

The decision to go forward with CJIS included a decision to increase and re-organize KBI staff. Chuck Sexson was made an Assistant Director and was put in charge of CJIS and the Information Technology Unit. He was told by the KBI Director that he would be given new staff, could reorganize the existing staff, and could do whatever he needed (attend conferences, purchase resources, etc.) to make the project work. Although there was some initial resistance to a sworn officer managing a civilian unit, employees eventually came around when they saw what a success CJIS was going to be.

Procurement Phase

RFP and Selection Process

Four RFPs were issued for the entire project. The first was for consultant services to conduct a needs assessment and develop the strategic plan. The other three were issued for the AFIS replacement, CJIS (to include the statewide network switch and the Central Repository initiatives), and the local system interfaces (see Attachment 3). A great deal of work and time went into the creation of the CJIS RFPs.³ Project staff, with the help of the consultant, went through an extensive standards process, defined CJIS requirements, and created a conceptual design.

All of the RFP processes included bidders' conferences, but site visits were done only for AFIS and CJIS. The AFIS project was also the only one of the four in which benchmarking was done. The consultant contract was awarded to MTG.

Eleven vendors were interested in the CJIS project during the pre-bid phase: PRC, Deloitte & Touche, Oracle, Hodges & Reed, SAIC, Bull Information Systems, CPI, Datamaxx, Printrak, IBM, and CCBS. Of these, four submitted proposals, and all were invited to an initial round of negotiations. One proposal was submitted by Paradigm4,

³ Note again that this case study is focused on the use of the intranet and will only touch briefly on the related projects.

and the other three were from vendor consortiums—Printrak/PRC/CPI, SAIC/Datamaxx/CPI, and Datamaxx/CPI. All except the Printrak group (which was too expensive and did not have the depth to take on CJIS in addition to everything else) were asked back for a second round of interviews.⁴

Upon further research, CJIS staff found issues with the costs, depth, and experience of both the SAIC and Datamaxx groups (although they still wanted to purchase Datamaxx's thick client terminals). The final decision was to award the switch and central repository contract (CJIS) to Paradigm4, with a smaller contract to Datamaxx for ASTRA end user software and hardware. Paradigm4 was chosen because they had previous experience in public safety; they were very conversant in the preferred technologies and environment; and they received a good reference from the state of Florida (for which Paradigm4 was building a system with similar technology).

Contract Negotiations

Kansas used a unique method, called “negotiated procurements,” for their contracting. Instead of the more common lowest bid or fixed price options, everything in the contract is negotiable except the scope of work. One word of caution from the Kansas experience was that the negotiation team must be very knowledgeable about the proposal and about contracts.

Because Paradigm4 was selected as the primary vendor, this included developing a number of subsystems as part of the larger CJIS. Paradigm was to provide the Message Switch (and backup), Central Repository, Justice Web Server, Public Access subsystem, system management tools, e-mail, and document imaging. Within the Central Repository, there are criminal history, an incident-based reporting system, transaction log, hot files, and customer and training information subsystems. The Justice Web Server allows authorized users to access Message Switch functions (NCIC, NLETS) and Central Repository data (CJIS, hot files, KIBRS). The Public Access subsystem will offer non-CJIS Internet users criminal history look-ups for a fee and access to road reports, missing persons, offender registration data, and crime reports.

Design meetings were held between Paradigm4 and all of the significant justice agencies, but especially with KBI and CJIS staff. This was considered to be a collaborative decision making partnership. The first design document was too broad, missed a lot of issues, and underestimated the schedule and number of staff-hours. A second design document was completed in September 1998, and although the number of hours was greatly increased, the Paradigm4 project manager still considered it an aggressive undertaking. Paradigm4 had eight to ten staff working full-time on CJIS, as well as two to three for specialized tasks. Since the re-design, they have been working diligently to stay under budget and within a reasonable time frame.

⁴ There were two proposals submitted for AFIS—Printrak and Morpho. Printrak was awarded the contract.

CJIS Security Acquisitions

The security side of CJIS was handled separately, using a sole source procurement option.⁵ In September 1997, the security design was accepted by the FBI, and KBI was able to begin buying equipment. Up until September 1998, the state standard CISCO equipment was still being strongly recommended over the proposed new options. Only two weeks before the new network was to be connected, KBI was finally able to get the more secure VPN approved. The sole source purchase was with Fishnet Consulting, a Kansas City company specializing in security systems. The implemented solution came about as a result of the CJIS Security Plan and an assessment of the various firewall and other available products. Fishnet could provide a packaged system, including the preferred CheckPoint firewalls, Internet Security Systems (ISS), and Entrust Technologies. In addition, Fishnet suggested products from several other vendors, including SecureID tokens by Security Dynamics (now RSA Security) and Netscape Directory Server.⁶

CheckPoint, with StoneBeat, provides redundant firewalls. SecuRemote, a client-side encryption software, provides the VPN. For an additional layer of security, the KBI uses Entrust Technologies, a two-key cryptography solution through a certificate authority server. The technology uses exchange of the public key (to encrypt the transmission from the server) and the private keys (to decrypt the messages on each receiver's workstation). Security Dynamics also supplies SecureID tokens to authenticate each user to a server. Finally, a digital certificate is needed to identify the public key, the name of the private key's owner, and other encryption information. KBI purchased the Netscape Directory Server to handle the digital certificates. The CJIS budget covered the initial costs for 4,000 tokens and 2,500 certificates. To monitor network traffic and detect suspicious or abusive use of the host or network, KBI included RealSecure and Internet Scanner by ISS in the Fishnet purchase.

System Hardware

The CJIS message switch (and its backup at the Highway Patrol Academy) is on a 200-MHz Dell PowerEdge 6100 Pentium Pro with 512MB of RAM using MS NT Enterprise. The primary message switch is located at KBI and resides on a 100MB LAN connected to the KBI LAN. The internal network was installed for \$108,000 and costs \$18,000 annually to maintain. A 10MB line connects KBI to the Kansas Division of Information Systems and Communications (DISC), who maintains the statewide frame relay network. Sites throughout the state can purchase any type of workstation that will support a LAN connection or modem. The CJIS project is responsible for purchasing routers and circuits so each of the 105 counties has at least one state-funded network connection. KBI will be administering the mail server that is housed at DISC, but it was still undecided who would administer the public server (also housed at DISC). The location and administration of the servers was an important issue.

⁵ Kansas policy states that any purchase over \$2,000 has to be bid, but an exception was made due to the uniqueness of the needs, the newness of the technology, and the urgency of getting the security in place ahead of the network migration to the Internet.

⁶ The KBI started out using Entrust Technologies for the certificates. Security Dynamics (now RSA) then came out with a competitive product. The KBI agreed to try their product and compare the results between the two. At the time of writing, KBI was using both Entrust and RSA.

KBI acquired the hardware for CJIS through the Paradigm4 contract. State software standards are Oracle and UNIX, and some of the prospective vendors proposed these as platforms. CJIS project staff opted for a less expensive and open system architecture so development could be the same for the majority of their “customers” (about 750, mostly very small agencies). They chose Microsoft SQL server, Windows NT, Exchange, and Visual Basic. They needed the cheapest, easiest, and yet inclusive products so local agencies could and would purchase them. Even though some KBI data processing staff were hesitant to leave their comfortable AS/400 environment and others wanted to be more consistent with the state standards, CJIS staff pushed for the lower cost and open architecture. They wanted to avoid vendors with proprietary applications and architectures that lead to difficult and costly maintenance and support. The hardware platforms for the chosen software environment were also much less expensive and were competitively available from more vendors than the UNIX/Oracle alternative.

As depicted in Attachment 2, there are multiple layers to the CJIS “network.” The Message Switch, Criminal Repository, CJIS Web, and Document Imaging servers are all connected to the KBI LAN. In addition, the Security System is also run through the KBI LAN. There are standard firewalls between KANWIN/Internet and “open” CJIS. There are additional DISC firewalls between the Public and Email Servers as well as “secure” CJIS.

Implementation Phase

Overall implementation started in 1997 and will continue through 2000. Some pieces of CJIS went into production in October 1998. The secure network went on-line in November 1998, and the CJIS web server in June 1999, but the majority of CJIS completion was planned for the fall of 1999. Local case and records management applications for law enforcement, prosecution, and probation officers were installed in a few sites on a pilot basis in December 1998 (see Attachment 3 for more detail). Full installations began in March 1999 and were scheduled to continue throughout the year. In total, KBI will provide a minimum 56K-circuit and router connection to more than 300 criminal justice sites in 105 counties.

Security Systems and Policies

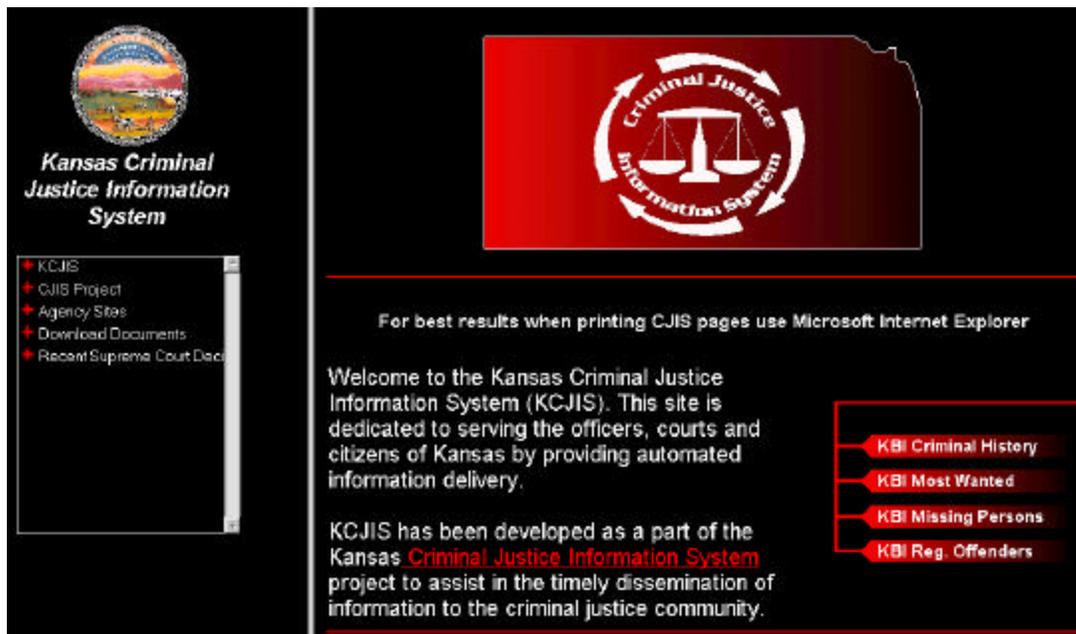
In September 1998, FishNet implemented a pilot installation of the CheckPoint and Technologies. KBI was the first agency to use the integrated products. Until that point, no agency had ever transmitted information via the Internet to NCIC because of the tight security restrictions. By November, the NCIC had amended its policies to permit Internet traffic and was convinced KBI had proper security in place under the new policies. The FBI gave its approval for the KBI to go forward. Further implementation of network security continues throughout the project as new subsystems have gone online.

The user security procedure is a four-step process. Each user has a SecurID keyfob token, about the size of a key chain, which gives the user a numerical password that changes every minute—it is based on two-factor authentication. It takes “something you have” and “something you know.” Once the ID and password are entered, a public encryption key is used for verification. Finally, the SecuRemote software encrypts and decrypts the data as it is transferred.

In an attempt to prevent accidental or purposeful abuse of the new systems, KBI instituted several new policies regarding security, network, and Internet use. The “KBI Personal Computer and Network Security Policies” is signed by all KBI employees who access KBI or KCJIS data. This ensures that each employee is aware of the computer usage policies and virus protection procedures, has a valid user account, and understands that activity can be tracked. The “Vendor Employee Computer and Network User Agreement” is signed by all employees of vendors and contractors who access KBI or CJIS data. This serves the same purpose as the previously described form. The “Acceptable Use of the Internet/Email” policy is designed so employees will be aware of appropriate and unacceptable uses, and of policies and procedures. This form is also signed.

Public Web Server

The Public Web Server was due to go on-line in June 1999 with full capabilities available by October, but has been significantly delayed while the underlying foundation work of the KBI’s Central Repository is finished. As of November, the CJIS web site (www.kbi.state.ks.us) offers access to the public only for general information (see below). One can view the mission and goals of the project or download a number of project documents, such as Requests for Proposal, Data Element Standards, Records and Reports Manuals, and Governance Membership Lists.



By clicking on the KBI Criminal History option, the following screen appears. This is the point where the user needs to enter the various secure IDs and passwords before going any further.



System Maintenance and Vendor Communication

The maintenance and support proposal received from Paradigm4 included having three people assigned to modifications, updates, software, and support for three years. In addition, KBI was hoping to negotiate an extended “warranty” because the project was behind schedule. CJIS staff believe that the biggest difficulties in the project timetable were establishing one before a design was done, not completing a valid detailed design, and failure of Paradigm4 to commit enough resources to achieve the proposed schedule. Although delayed, CJIS staff are happy not only with the products, but that Paradigm4 is honoring the fixed price nature of the contract. Paradigm4 suggested that project implementation could have gone smoother if several things occurred. They would have liked better communication between vendors; and they felt there was a lack of timely responsiveness between vendors. They also felt the customer should have been a more aggressive mediator between the numerous vendors on design and other scope issues.

Marketing and Training

While original “marketing” of this type of project began in 1993, active education and training for CJIS began in August of 1998. A mailing went out to all users, and approximately 500 representatives from local agencies attended a series of three conferences held at the Kansas Highway Patrol (KHP) Academy in Salina. The conferences were one or two days each and had training and breakout discussion sessions. The first conference’s focus was “here’s what’s coming,” the second covered technical issues, and the final one had more technical issues and an installation schedule. A fourth conference was conducted strictly on security; KBI wanted to answer

the questions of “how do I know if I’m secure?” and “how will my network interface?”⁷ In addition, a series of six regional sessions were held throughout the state in December 1998 to demonstrate the local applications and update agencies on the project status. The first round of training finished in February 1999. Web-based training was due to start in the summer of 1999.

In November 1998, Paradigm4 and BSE trained KHP and KBI staff in many of the products and tools that will be used to manage and enhance the systems. This type of training will continue throughout the project. The Highway Patrol has done the training on the Datamaxx terminal interface and will be doing the Paradigm application functionality training as well. They are using a “train the trainers” approach, so each agency is sending one or two people.

Staffing

Additional KBI technical staff were hired for the implementation of CJIS. Key people include an Information Resource Manager and an information technology expert to handle security issues. The KBI Information Technology Unit now has six people. In addition, the hotline and field auditing staff had some paperwork reduced and were then re-trained (on the job) to provide a Help Desk for IT issues (six people) and security (two people). One employee remains to handle the traditional functions. The questions have ranged from “how do you turn on the computer?”⁸ to very technical programmatic issues. Some customers had problems at the beginning, but as the project has progressed, the Help Desk service has been improved. They also put together a Frequently Asked Questions handout.

Interface with Regional Justice System (ALERT)

Another CJIS implementation issue that the state faced was the need to interface with ALERT, the existing Kansas City regional justice system that serves more than one-quarter of the state’s population (as well as part of Missouri’s population). In addition to the bi-state nature of the system, there were other technical as well as political obstacles to overcome. Although many have been overcome, CJIS staff realizes there will continue to be related challenges in the future.

Impact Phase

In one year, the KBI went from ten micro-computers and a bunch of dumb terminals to a new network and 150 micro-computers. Similar impacts occurred in almost all the other agencies involved in CJIS activities at both the state and local levels. As of March 1999, CJIS was available to 250 Kansas law enforcement offices with 4,000 employees, and they expect to reach 750 offices with 12,000 law enforcement officials by the end of the year (Korzeniewski, 1999). The KBI Director summed up the project’s impact when he

⁷ Unfortunately, many locals had no idea what their network even looked like and wanted KBI to assist. There were not enough KBI staff to support all of the requests, and they recommended to the locals to hire security expert consultants.

⁸ When the Help Desk employee responded, “Didn’t you attend training?” the befuddled officer said, “Yes, but the computers were already on.”

stated, "Four years ago, Kansas ranked at the bottom of criminal history—we were a joke. Now, Kansas is the only state allowed to send FBI criminal history information through the Internet."

Benefits for State and Local Agencies

KBI agents have experienced great benefit from the new network. They are able to quickly collect information and graphics that were previously inaccessible. A couple of years ago, an officer or agent needing a criminal history record from the KBI had to mail in a request, receiving a written response several weeks later; the result now can be downloaded in about three minutes (if the record is complete and automated). Besides timeliness, other benefits being realized by the state include improved accuracy, reduced paper and paper handling costs, low-cost data circuits (Internet), fast statewide communication (via email), image transferability, off-site backup, and security awareness and protection. In addition, there have been and will be numerous benefits to local jurisdictions. These include faster, accurate reporting; access to new data; free email; faster, low-cost circuits; image retrieval; Livescan capability; and off-the-shelf components (Schaefer and Rohr, 1999).

Challenges

There were a number of challenges faced in implementing CJIS (Schaefer and Rohr, 1999). Funding projections and sources were estimated accurately except for the high-level security.⁹ In addition, there were unplanned annual maintenance, staffing, and security consultant costs at the state level. At the local level, there were unanticipated hardware/software acquisition costs and security outsourcing. Many of the locals had no idea what they needed or how to manage the new system. Because there were so many agencies involved in the project, there were turf issues regarding location of systems and maintenance of data. Because so few people and agencies had email in the planning stages, communication was difficult and costly. Finally, deployments of the systems throughout the state and new support responsibilities were also obstacles that needed to be overcome.

Key Factors for Success

Even with the plan and governance structure, some feel that CJIS was just too big to implement as one project. Instead of tackling the whole thing at once, they believe, it would have been easier to develop subsystems individually. The enormity of the one system was a drain on staff, and communication with and collaboration between multiple vendors was difficult. Another lesson learned was that the funding entity should be heavily involved in the project (the Sentencing Commission managed all of the grants and distributed the money but was not an active player). Although some interviewed felt there were very few turf battles between Advisory Board members, others noted that the CJAB mitigated several of these battles—often between historical combatants. With respect to support, the courts generally supported Phase 1 for law enforcement and hope law enforcement will, in turn, continue to support the courts during Phase 2.

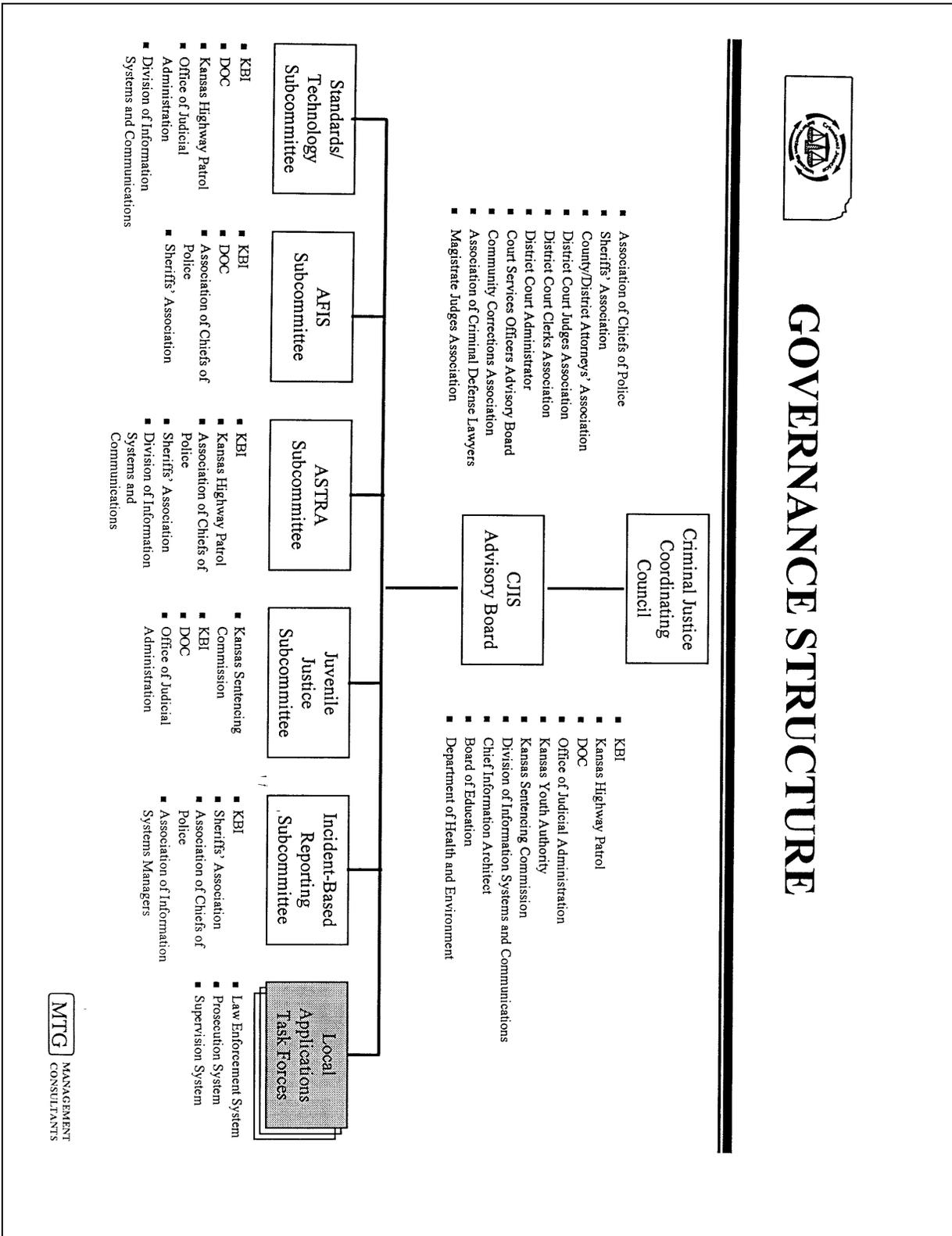
⁹ The initial budget was \$18,000 for one firewall, while the final cost of the security system was \$485,000.

Several people involved in the project attribute at least part of the success to the strategic plan. They feel it kept them on track and gave them direction. Another reason for the success was that it was well financed. Besides grant money, the Legislature saw the need and was willing to spend a large amount of the state's money.¹⁰ Lastly, others attribute the success (and would recommend this to others tackling large-scale projects) to the governance structure and quick successes for customers. The governance structure, set up across agencies, kept in mind the project's impact on the needs of everyone involved, such as keeping the cost down for locals and the availability of information for citizens. The quick successes gave the customers results and not just promises, which allowed for better buy-in.

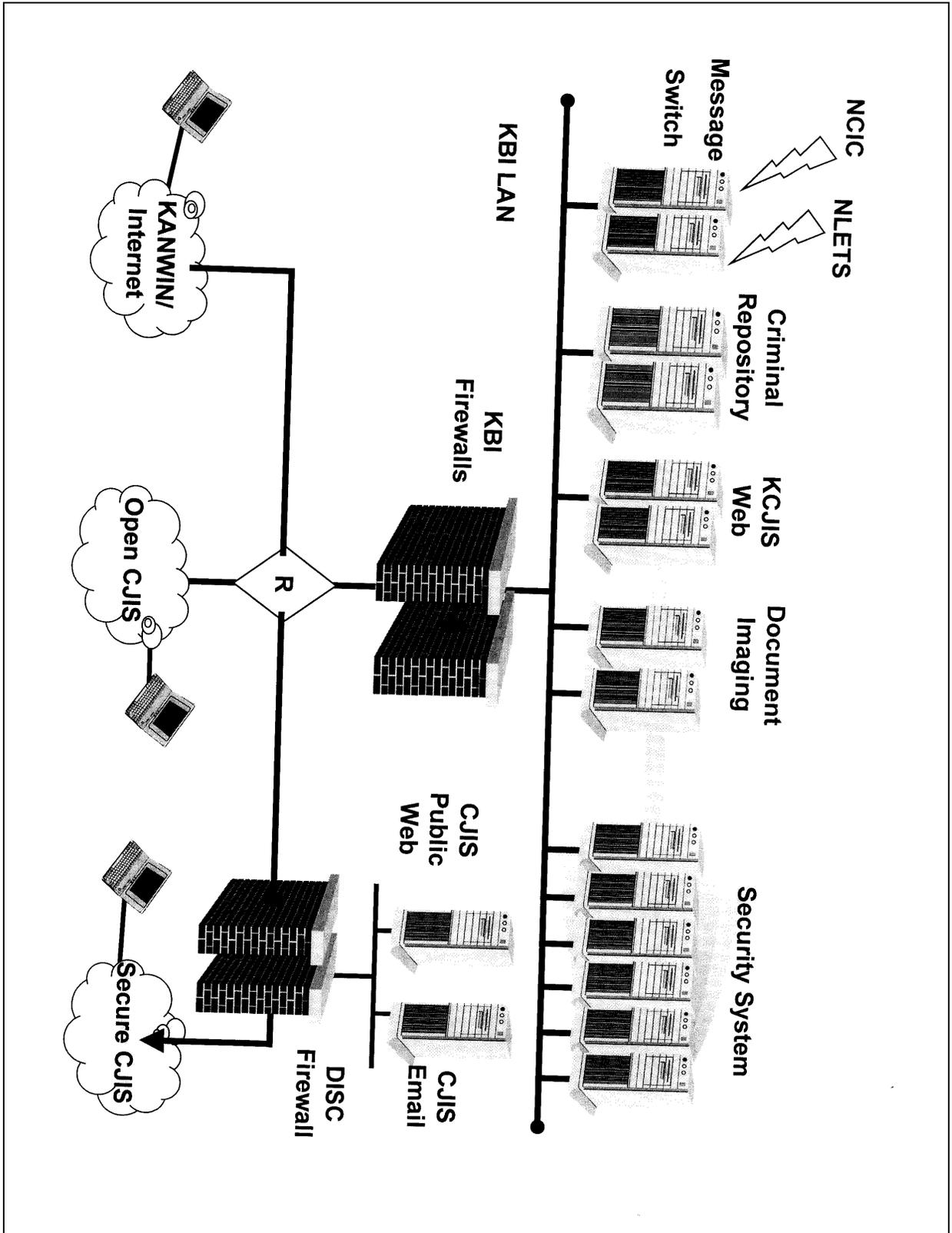
¹⁰ Funding was a big issue in 1999 and is again this year as different entities try to re-allocate state funds to other areas, especially in extremely tight times.



GOVERNANCE STRUCTURE



Attachment 2



Attachment 3: Local Application

Assessment and Decision Making Phase

One goal of CJIS was to address needs of the local agencies while fulfilling the state's need to receive electronic submission of CJIS information. The idea was to create local applications for law enforcement, prosecution, and supervision to interface with the statewide CJIS. KBI's first, unsuccessful attempt to get information from the local agencies lasted from 1989 through 1993. That effort was largely unsuccessful because it offered little that helped local agencies. The primary difference with the current CJIS project was that the local agencies were involved from the beginning. Users had input, and the new system would benefit the officers and agencies in addition to benefiting KBI by eliminating some of the latter's data entry load.

The original plan was to create a system for the small agencies—the majority of law enforcement, prosecution, and probation entities in Kansas.

Procurement Phase

The local applications contract RFP was released in mid-1997, and three vendors submitted proposals. They were Business Software and Equipment (BSE), CTA, and a small family business that had done programming for local justice agencies in Kansas. It was not feasible for the small firm to take on such a huge project. CTA came in with a high cost and no previous experience. Although BSE did not have criminal justice experience, they had done client-server work and TCP/IP applications across multiple jurisdictions and proposed a reasonable price. The contract was awarded to BSE in the summer of 1998.

BSE and the state put together separate design teams for each of the applications. Some groups went more smoothly than others. Users on the design teams pushed for more functionality than the original RFP specifications, and BSE agreed to deliver some of the items. Getting the users' buy-in during the design stage was imperative to creating a successful system. The local system was created in Microsoft Access, but some of the larger agencies (who were not included in the original plan) saw the system and wanted one, too. BSE was awarded a separate contract in the fall of 1999 to develop a similar application in Visual Basic/SQL Server for the larger jurisdictions.¹¹

BSE felt that the original RFP schedule was unrealistic and negotiated a new one. They worked with selected agencies throughout the state to implement the initial interface but also had to work within certain development constraints based on Paradigm4's progress. Because the overall project was so complex and had multiple committees, vendors, and new policies, minor changes caused massive delays. Some of the delay was caused by the inter-linking aspect of the applications and the fact that they shared a common code base for the core of each version. BSE had 15 people working on the project at various times.

¹¹ The original MS Access-based version could not support enough users to work in larger agencies. The Visual Basic/SQL Server-based version should be deployed during the spring and summer of 2000.

Implementation Phase

Local applications for law enforcement and prosecution were installed in a few sites on a pilot basis in December 1998. Although KBI was using their web site and other marketing tools such as newsletters to police chiefs and associations, and had visited six geographically dispersed sites for demonstrations, some agencies were still not aware of the project and its progress. Full installations began in March 1999 and were scheduled to go throughout the year, depending on the demand. In total, the state will provide a 56K circuit with router connection to each of the 105 counties in Kansas. Those connections, plus ones paid for directly by additional agencies as part of the network upgrade, will also serve as the path for electronic data submission. Local law enforcement is presently sending the information to KBI via EDI/Secure Socket Layer (SSL) transmissions.

The state covered the cost of the application, but the jurisdictions were responsible for buying hardware and other necessary software (such as Microsoft Office), installing the software, and restructuring their networks. Based on pricing from DISC, KBI had promised the locals that network connections would cost them \$365 per month, but in the end it turned out to be higher. While Byrne grant money (\$277,000) has covered the excesses for the first year, CJIS is trying to find a way to continue to make the project cost effective for the locals. Some of the local jurisdictions are using separate grant money to fund hardware and network modifications.

Training and installations were done regionally. Training for law enforcement lasted two days—one and one-half days on the application functionality and a half-day on system administration. Computers were transported in a trailer, and a hotel classroom was used for 15 students at a time. The state paid for one person to be trained from each installing agency, and agencies can pay to send additional people.

BSE provided a one-year warranty for the software, starting with delivery of the software to the state, but had not yet negotiated a maintenance or upgrade contract. Several agencies noted BSE was very responsive and customer-oriented and had provided “corrections” to the system as needed. As part of the original contract, the state has an unlimited license to distribute the software to any agencies within the state and shares ownership of the applications. The state strongly encourages agencies going to new applications to use BSE, and future modifications and upgrades will be through BSE. The state, because it has ownership, could provide the code to someone else if BSE were to no longer support the applications.

Impact Phase

One accomplishment of the CJIS-local law enforcement project was to bring the state and local agencies into a partnership. In the past, it was often the state telling the locals what they had to do, what they had to buy, and how to do it. With CJIS, the locals were able to have a voice in the governance structure, input in the design of their applications, and a smooth process of communicating information. Many people interviewed agreed that the project would not have succeeded had they not obtained input from users at all levels of the local agencies. One person added that it was a cost and ease of use benefit to give the local agencies the ability to make acquisitions through blanket state contracts and purchase orders.

Local agencies had various reasons for wanting the new BSE application. Some did not have a computerized records management system, others wanted a more user friendly system for officers and records clerks, and some valued the ease of data transfer to KBI. The system was still relatively new to most agencies and each was finding benefits in different ways. One of the larger jurisdictions was concerned with the robustness of the application, but was looking to test it and get upgrades over the year. They were really enjoying the new ease of transfer of data—getting it out of Access rather than a proprietary system.

References

- Kansas Bureau of Investigation, CJIS Initiatives Status spreadsheet, 1999.
- Kansas Bureau of Investigation, Vendor and Employee Computer Agreements, 1999.
- Kansas Criminal Justice Coordinating Council Information Systems Subcommittee, CJIS Criminal History Record Improvement Plan, 1995.
- Kansas Criminal Justice Coordinating Council, Governance Structure Chart, 1999.
- Kansas Criminal Justice Coordinating Council, CJIS Resource Directory, 1998.
- Kansas Division of Information Services and Communications, various network diagrams, 1999.
- Kansas Legislature, copies of Article 57 (1992) and Article 95 (1997).
- Kansas Office of the Attorney General, various CJIS budget spreadsheets and charts, 1999.
- Korzeniowski, Paul, "Virtual Network Lets Law Enforcement Agents Swap Secure Case Files," *CNN Interactive*, March 22, 1999.
- MTG Management Consultants, State of Kansas Criminal Justice Information System Strategic Plan, 1997.
- MTG Management Consultants, State of Kansas Criminal Justice Information System Project Overview, 1998.
- Paradigm4, Public Safety Solutions Primer, Integrated Justice Information Systems, Kansas ASTRA Re-engineering System, 1999.
- Schaefer, Norma Jean and Ron Rohrer, Kansas Bureau of Investigation, Presentation slides on CJIS Security System, 1999.
- Sexson, Charles, Kansas Bureau of Investigation, Reports on Central Repository and Records Improvement Project, 1996.
- Walsh, Trudy, "FBI OK's Kansas' online links," *Government Computer News*, December 1998.

Contact Information

J. Carey Brown
Criminal Justice Information System Director
State of Kansas, Office of Attorney General
brownjc@at02po.wpo.state.ks.us
(785) 296-7266

Table of Contents

Background on the Project	1
Role of the Coordinating Council and Advisory Board	1
Report Organization	2
Summary of the Technology Solution	2
Assessment and Decision Making Phase	3
Problem Statement	3
Records Automation Project	3
CJIS Strategic Plan	3
Data Accessibility and Management Needs	4
Options Considered	5
Project Organization and Staffing	5
Procurement Phase	5
RFP and Selection Process	5
Contract Negotiations	6
CJIS Security Acquisitions	7
System Hardware	7
Implementation Phase	8
Security Systems and Policies	8
Public Web Server	9
System Maintenance and Vendor Communication	10
Marketing and Training	10
Staffing	11
Interface with Regional Justice System (ALERT)	11
Impact Phase	11
Benefits for State and Local Agencies	12
Challenges	12
Key Factors for Success	12
Attachment 1: Governance Structure	14
Attachment 2: CJIS "Network"	15
Attachment 3: Local Application	16
References	19

