U.S. Department of Justice
Office of Justice Programs
Bureau of Justice Assistance

BJA

Bureau of Justice Assistance

Keynote Presentations: 1999 Symposium on Integrated Justice Information Systems

Monograph

U.S. Department of Justice
Office of Justice Programs
810 Seventh Street NW.
Washington, DC 20531

Janet Reno
Attorney General

Raymond C. Fisher
Associate Attorney General

Laurie Robinson
Assistant Attorney General

Noël Brennan
Deputy Assistant Attorney General

Nancy E. Gist
Director, Bureau of Justice Assistance

Office of Justice Programs
World Wide Web Home Page
www.ojp.usdoj.gov

Bureau of Justice Assistance
World Wide Web Home Page
www.ojp.usdoj.gov/BJA

For grant and funding information contact
U.S. Department of Justice Response Center
1–800–421–6770

This document was prepared by SEARCH, The National Consortium for Justice Information and Statistics, under grant number 97–DD–BX–0077, awarded by the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice. The opinions, findings, and conclusions or recommendations expressed in this document are those of the authors and do not necessarily represent the official position or policies of the U.S. Department of Justice.

The Bureau of Justice Assistance is a component of the Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, and the Office for Victims of Crime.

BJA

Bureau of Justice Assistance

Keynote Presentations: 1999 Symposium on Integrated Justice Information Systems

August 1999

Monograph

NCJ 178231

Foreword

Justice agencies at the federal, state and local levels have long recognized—and embraced—the benefits of information technology as a tool to fight crime, ensure public safety, and provide accurate, complete and timely information on offenders and their status in the justice system. In the past few years, justice information technology priorities have shifted to the next level of automation: integration. Integrated justice information systems improve the ability of justice agencies to share information on an interagency, interjurisdiction, or multijurisdiction basis.

Integration offers enormous benefits: reductions in redundant data entry, decreased storage costs, and higher quality justice made possible by swift and valuable information exchanges. Before justice agencies can fully reap these benefits, however, they have to successfully surmount a series of challenges unique to government and public agencies, such as multiple-year funding cycles; security, privacy and confidentiality issues; turf battles and data ownership; and governance structures and the needs of stakeholders.

To address the opportunities, solutions, and challenges facing justice system integration, the Bureau of Justice Assistance (BJA), U.S. Department of Justice, and SEARCH, The National Consortium for Justice Information and Statistics, sponsored the *1999 Symposium on Integrated Justice Information Systems* in Washington, D.C., February 8–10, 1999. The symposium was designed to provide practical resources to agency executives, managers, and technologists in state and local justice agencies who are considering or are in the midst of implementing integrated justice information systems. More than 60 experts from government agencies, nonprofit organizations, and the private sector shared strategies for successful integrated systems planning and implementation.

The symposium was an enormous success. More than 1,000 justice agency professionals representing courts, correctional agencies and jails, and law enforcement, public defense, prosecution, and other agencies from 49 states, the U.S. Virgin Islands, Puerto Rico, and several foreign countries attended. I believe this is a testament to justice agency interest in learning how to plan for, implement, manage, and secure integrated justice information systems. For the first time, “teams” of justice practitioners from state and local jurisdictions attended; the participation of these teams, which ranged in size from 4 to 33 individuals, helped cultivate and organize relationships between agencies and individuals in planning for the integration of their information systems.

This publication includes the keynote and plenary presentations delivered at the 1999 symposium. To access the presentations of many of those who addressed breakout sessions, visit the symposium World Wide Web site at www.search.org/1999symposium.

I am confident that this publication and the online resources created for the symposium will prove invaluable to those agencies that are planning or in the midst of efforts to integrate their information systems with local, county, regional, state, or federal counterparts in the criminal justice system and to those agencies that are maintaining installed systems. The combined experiences and expertise contained herein provide a useful reservoir of information gathered from individuals with years of experience in criminal justice and in justice information technology. Their perspectives provide an important foundation on which to observe the rapidly changing and always evolving world of information technology.

Nancy E. Gist
Director

Acknowledgments

The *Keynote Presentations: 1999 Symposium on Integrated Justice Information Systems* report was produced by SEARCH, The National Consortium for Justice Information and Statistics. Mr. Kenneth E. Bischoff is the Chair and Mr. Gary R. Cooper is the Executive Director of this private, nonprofit consortium of the states.

Production of the report was supervised by Mr. David J. Roberts, Deputy Executive Director. Support was provided by the following SEARCH staff: Ms. Kelly J. Harris, Director of Justice Information Technology Services; Ms. Twyla R. Cunningham, Manager of Corporate Communications; Mr. Eric C. Johnson, Policy Research Analyst; and Ms. Jane L. Bassett, Publishing Assistant. The project was conducted under the direction of Mr. José McLoughlin, Grant Monitor, Bureau of Justice Assistance.

Contents

Welcoming Remarks 1

Nancy E. Gist
U.S. Department of Justice

Keynote Address 5

United States Attorney General Janet Reno

Keynote Address 11

United States Senator Mike DeWine

Improved Criminal Justice Through Information-Sharing: Office of Justice Programs' Justice Integration Initiative 15

Paul F. Kendall
U.S. Department of Justice

Integrated Justice Information Systems Planning and Implementation: Organizing for Change 21

David J. Roberts
SEARCH, The National Consortium for Justice
Information and Statistics

Creating a Community of Value Around Criminal Justice: Digital Strategies for Funding Integration Efforts 31

Steve E. Kolodney and Paul W. Taylor
Washington State Department of Information Services

Technology Issues and Challenges 39

Robert L. Marx
SEARCH, The National Consortium for Justice
Information and Statistics

Managing the Integrated System for the Long Term 47

Paul Leuba
IBM Corporation

Criminal Justice Information Privacy 59

Robert R. Belair
Mullenholz, Brimsek & Belair

Securing the Integrated Kansas Criminal Justice Information System 73

Norma Jean Schaefer and Ron Rohrer
Kansas Bureau of Investigation

Nancy E. Gist is Director of the Bureau of Justice Assistance (BJA), U.S. Department of Justice (DOJ). Ms. Gist was sworn into office on October 20, 1994, following confirmation by the U.S. Senate.

Before joining DOJ, Ms. Gist served as Deputy Chief Counsel of the Massachusetts Committee for Public Counsel Services in Boston, a post she held since 1984. She is nationally recognized for her pioneering work in the development of prepaid legal service delivery systems and for her innovative work in the area of indigent defense.

Prior to 1984, Ms. Gist spent 7 years as Director of Midwest Legal Services and Assistant Director of the United Auto Workers Legal Services Plan in Detroit. For almost 4 years Ms. Gist also served as Staff Attorney at the Chicago Lawyers' Committee for Civil Rights Under Law.

As BJA Director, Ms. Gist is responsible for administering the primary criminal justice grant agency of the DOJ. In fiscal 1998, $1.7 billion was appropriated for BJA activities to support collaborative efforts in every area of the criminal justice system, including law enforcement, crime prevention, corrections, courts, prosecution, probation, indigent defense, pretrial services, technology (with a special emphasis on integration), evaluation, and training and technical assistance.

Born and raised in Chicago, Illinois, Ms. Gist received her J.D. from Yale Law School in 1973, and her B.A. in economics from Wellesley College in 1969.

Welcoming Remarks

By Nancy E. Gist
Director, Bureau of Justice Assistance
U.S. Department of Justice

I am delighted to be here today and welcome all of you to our nation's capital, Washington, D.C., and on behalf of the Bureau of Justice Assistance (BJA) and the other offices and bureaus of the Office of Justice Programs, U.S. Department of Justice, we welcome you to the *BJA/ SEARCH 1999 Symposium on Integrated Justice Information Systems*.

I have the distinct pleasure of addressing this symposium, and meeting with you at this dynamic event, which will provide practical resources to state and local agency representatives like yourselves who are considering or are in the midst of implementing integrated justice information systems. This is a very exciting time for integration and information technology, considering the progress we have made and the bright future which faces us as criminal justice practitioners. As we stand at the threshold of a new millennium, exciting opportunities await our nation's justice agencies as they move toward the advanced automation and integration of their information systems. Technology is changing the way we are doing business in the justice system.

This *Symposium on Integrated Justice Information Systems* brings together practitioners, policymakers, administrators and researchers: a cross-section of criminal justice professionals to share information on the rapid advancements in technology and other impact issues related to justice information integration.

Information technology has become a powerful crime-fighting tool. Justice agencies rely on instant access to critical information about offenders and their status in the criminal justice system. Judges rely on up-to-date criminal histories to sentence offenders appropriately, police officers can now obtain a suspect's outstanding warrant history via computer in the patrol car, and corrections officials use information technology to positively identify inmates before release.

Clearly, computerized access to accurate and timely information about those who come into contact with the justice system is paramount to the swift and fair administration of justice.

This conference is truly one of a kind in that it is geared toward agency executives, managers and technologists who will focus on issues such as funding and managing integrated systems, evaluating new technologies for justice integration, developing system standards and identifying best practices.

This 1999 symposium, therefore, comes at a very opportune time. Three years ago, BJA and SEARCH hosted the *1996 Symposium on Integrated Justice Information Systems*. That event drew national attention to the importance of systems integration, and laid the foundation for enhancing justice system connectivity. Three years later, we are experiencing a culmination of several major events that, working together, have placed justice system integration near — if not at the top — of local, state and federal government information technology priority lists.

Since 1996, information and communications technology has altered the face of criminal justice, and BJA and other federal agencies have played a key role in the integration initiative. BJA and its sister components within the Office of Justice Programs (OJP) provide assistance to state and local governments through grant programs designed to foster partnerships to improve the criminal justice and juvenile justice systems nationwide.

As part of this mission, BJA and OJP have long acknowledged the need to assist state and local governments in the development of criminal justice information-sharing capabilities, and have demonstrated a clear vision of improving criminal justice information systems. This vision includes an array of programs that support the creation of a nationwide network of criminal justice information systems where state and local stakeholders with responsibilities for law enforcement, courts, prosecution, corrections, probation, parole and public defense have immediate access to all information necessary to respond to and resolve crime. In the Fall of 1997, OJP recognized the need for an intergovernmental architecture that facilitates the interoperability of locally autonomous criminal justice information-sharing systems, and created the Information Technology Executive Council.

BJA has also played a major role in facilitating the development of integrated criminal justice information-sharing systems. In the Fiscal Year 2000 budget, BJA has requested to assist the Executive Council by administering peer-to-peer consulting at the state and local level, information system strategic planning assistance, and “pilot projects” in which BJA will enhance already successful integration initiatives and use these projects as “learning laboratories” for other states.

BJA and OJP are planning to further assist jurisdictions in order to effectively and efficiently meet the increasing demands of information technology and the integration of information-sharing systems.

During 1998, OJP hosted three Intergovernmental Information Sharing Meetings, bringing together teams from 25 states to solicit information from local- and state-level justice practitioners about integrated information systems planning and implementation. These meetings have showcased the importance of integrated systems planning and implementation, and have provided guidance to OJP and to BJA on the kinds of resources that will assist local, state and federal integration initiatives.

BJA, through our formula, block and discretionary grant programs, is encouraging the implementation of innovative technologies that will meet the needs of user agencies. BJA is also encouraging information-sharing and integrated justice through many technical assistance initiatives. Within the State and Local Assistance Division, The Investigative and Surveillance Technology Initiative is attempting to achieve new means of helping you acquire and use the best possible technology. Therefore, the Institute of Investigative Technology will design and deliver training in the use of investigative and surveillance technology to approximately 3,500 state and local law enforcement officers throughout the United States as part of the BJA Technical Investigative Training Program.

The justice community is at a historic turning point with regard to integration efforts. New funding sources are dedicated to justice system integration, rapid advances have been made in technology, the public demand for more complete and timely information has increased, and the Attorney General is fully committed to justice system integration.

One of the most exciting events of late was the President’s signing of the *Crime Identification Technology Act of 1998,*[1] passed by the Congress and effective this year. This legislation authorizes $250 million per year for each of the next 5 years ($1.25 billion total) for state grants to promote the integration of justice system information and identification technology. The new law is intended to permit all components of criminal justice (law enforcement, courts, public defense, corrections and prosecution) to share information and communicate more effectively on a real-time basis.

Attorney General Reno has recognized the importance of integrated information systems

[1] Pub. L. No. 105-251 (1998).

strategic planning and coordination. As she pointed out during the *1996 Symposium on Integrated Justice Information Systems*, "as useful as computerized information may be, we fail to even scratch the surface of its potential if we don't move towards integration through strategic planning."

Although we have made great strides over the last few years in helping the justice community take advantage of state-of-the-art information technology, the road to integrated systems implementation is still lined with many challenges, such as funding needs that transcend traditional acquisition procedures and bureaucratic boundaries, potential conflicts between public access, privacy and confidentiality, security issues and the need to develop acceptable information exchange standards and long-term system maintenance plans.

These and other challenges to integration will be addressed during the next 3 days.

I have witnessed the power of information-sharing and how you, the information technology executives, managers and technologists of this nation, can use integration to combat criminal activity. Over the next several days, you will be talking, exchanging ideas and opinions, and searching for the information necessary to make your goals as criminal justice personnel attainable. It is our expectation that the information being exchanged and learned throughout this conference will translate into a better understanding of practices, challenges, policy, legislation, prosecution and defense issues, and education of integration. Enjoy the conference and take as much information with you as possible and use it to educate your communities, your schools, your civic leaders, your business leaders and, most importantly, your children.

As Attorney General Reno stated at the 1996 BJA/SEARCH symposium, "technology can help to keep our neighborhoods safe; it can solve crimes. Let us work together to make sure that we master the technology and that we master it in a way that makes it consistent with our Constitution and with the principles of this nation, as we use it to protect our citizens and our communities."

These are truly words to take with you throughout this symposium and back to your jurisdictions. Thank you.

Janet Reno is the first woman U.S. Attorney General. She was nominated by President Bill Clinton on February 11, 1993, sworn in a month later, and reappointed by the President in 1997.

Attorney General Reno attended public school in Dade County, Florida, and in 1956, she enrolled at Cornell University, where she received a bachelor's degree in chemistry. In 1960, she enrolled at Harvard Law School, one of only 16 women in a class of more than 500 students. She received her LL.B. from Harvard 3 years later.

In 1971, Janet Reno was named Staff Director of the Judiciary Committee of the Florida House of Representatives, where she helped revise the Florida court system, and in 1973 she was named Counsel for a state Senate committee responsible for revising the Florida Criminal Code. In 1973, she accepted a position with the Dade County State Attorney's Office, where she organized a juvenile division. She left the office in 1976 to become a partner in a private law firm.

In 1978, Janet Reno was appointed, and later elected, State Attorney for Dade County. The voters returned her to the office four more times. Juvenile justice system reform, pursuit of fathers for child support payments and the establishment of the Miami Drug Court and a career criminal unit were some of her accomplishments while serving as State Attorney.

Keynote Address

By United States Attorney General Janet Reno

(**Editor's Note**: Prior to her address, U.S. Attorney General Janet Reno was awarded the 1998 *O.J. Hawkins Award for Innovative Leadership and Outstanding Contributions in Criminal Justice Information Systems, Policy and Statistics in the United States* by SEARCH Chairman Kenneth E. Bischoff.[1])

I would like to express my thanks to you all. It is an extraordinary honor for me to receive this award and, particularly, to have Mr. Hawkins here when I receive it. I have admired the work that he does so very much.

The award should actually go, however, to some really wonderful and dedicated people in the U.S. Department of Justice. I could not begin to do this job by myself. I would not understand it all. I want to recognize so many different people who work in the Justice Department, in the Office of Justice Programs (OJP), in the Justice Management Division, and in the Federal Bureau of Investigation. They are extraordinarily dedicated people. One of my missions while I am Attorney General and even after I leave the office is to let the American people know how many wonderfully dedicated people work with them and for them in the Justice Department.

One of those people is Ms. Nancy Gist, Director of the Bureau of Justice Assistance (BJA), who is here today. I thank you, Nancy, for your leadership at BJA, and for all that you are doing to advance us into the next century in terms of criminal justice technologies and initiatives.

I have admired SEARCH from afar, and I have seen its work up close. I am gratified by the contributions of the National Technical Assistance and Training Program, which SEARCH directs under funding from BJA.

In addition to this symposium, the SEARCH program has provided invaluable training and technical assistance to so many justice agencies across the country. I can tell you from first-hand experience how valuable such training can be. As a state attorney trying to initiate the first steps of an information system, I know how difficult it is. You start, you test, you back up, you think that you have not done it right, and then you start over. It is invaluable to have an organization such as SEARCH with the answers, so that you do not make the same mistake twice.

The technical assistance and training program is another example of how partnerships — here a partnership between BJA and SEARCH — can yield dramatic results.

[1] The *O.J. Hawkins Award*, the highest bestowed by SEARCH, recognizes an individual's contributions to improvements in the criminal justice community's ability to develop and use information. It has been awarded every year since 1985. The award is named for O.J. Hawkins, SEARCH's first Chair and Executive Director, who was present for the Attorney General's address.

I would also like to recognize the critical role played by SEARCH in so many important national programs and initiatives, such as the *National Crime Prevention and Privacy Compact*, the National Criminal History Improvement Program (NCHIP), the Global Criminal Justice Information Network, and the National Incident-Based Reporting System (NIBRS) program. Under the leadership of SEARCH Chairman Kenneth E. Bischoff, and pursuant to the efforts of so many people, SEARCH's assistance in all these programs and initiatives has been invaluable. You are giving me credit for guidance on the development and implementation of NIBRS when I should just give the credit to all of you.

I came to Washington, D.C., wondering what it would be like after having served as State Attorney in Miami for 15 years. You get to know your public defender, your courts, your correctional system, and then you come into a whole new world of multiple correctional systems, hundreds of police agencies, and many different courts.

Despite the different environments, the principles are the same: How do we work together? How do we cooperate on matters of judicial administration? There are so many ways we can do that. A partnership is absolutely essential.

Nancy told me as I came in today about the number of teams that are here at the symposium. For prosecutors, public defenders, judges, correctional officials and law enforcement officials to be here together as teams is an extraordinary step. I commend you. We have an opportunity when people come together in this fashion to really make a difference.

The United States' Violent Crime Rate fell almost 7 percent in 1997. It has fallen more than 21 percent since 1993. Violent crime rates are at their lowest levels since 1973, when the Bureau of Justice Statistics began its National Crime Victimization survey.

These are exciting numbers, but I know full well from my experience that there is a tendency in America to say that crime is down and everything is okay. We become complacent, and the crime rate starts back up, or a new insidious substance such as crack cocaine comes on the scene, or some other force is brought to bear.

We cannot become complacent. SEARCH, and all that it stands for, can lead the way in keeping the pressure on. If we use the precious information available to us now through modern technology in partnership to make the system work better, and if we use it to make the system more effective and responsive by pooling information to solve crimes and to effect appropriate sentences, we can have a dramatic impact on the culture of violence in this country.

Toronto had about 100 gun homicides from about 1993 to 1998. Chicago, a city of similar size, had some 3,000 gun homicides in the same period. We do not have to be violent in this country. With the spirit and cooperation in this room, and with the emphasis on fact, on information and on what is happening, we can truly make a difference.

I urge you to continue your efforts, and to renew your efforts, for they can indeed make a difference.

One of your efforts, along with that of United States Senators Mike DeWine (R-Ohio) and Patrick Leahy (D-Vermont), has been the enactment of legislation in the area of information collection and sharing.[2] This is an excellent example. With the technologies now available, why do we have to maintain a federal criminal information system and 50 different state systems? Can we share some of these technologies in an appropriate way to avoid duplication, to avoid fragmentation, and to avoid the cost inherent in these technologies?

Former President Dwight Eisenhower gave a wonderful farewell address as he left office that has been obscured in history, but I recommend it to you all. He warned of the military-industrial complex and the influence that it would have on America for a long time to come.

We have to work with those who produce technologies to make sure that the industrial law enforcement and correctional complex works together, not to raise costs and not to require the purchase of a new piece of equipment every year because the old one has become obsolete, but so we use our precious resources wisely to develop technology that works.

[2] *Crime Identification Technology Act of 1998*, Pub. L. No. 105-251, was passed by the Congress and signed into law by President Clinton in October 1998.

I think this effort can be so very important. In his budget for Fiscal Year 2000, the president included $350 million to help state and local law enforcement agencies tap into these new technologies. This program includes $50 million under the *Crime Identification Technology Act*. Using this money, states will be able to upgrade their criminal history and criminal justice record systems and integrate with federal, state and local information systems, to name just a few of the possible purposes. The president's program also contains an additional $20 million for the Global Criminal Justice Information Network initiative. Again, I thank you for what you have done to promote this initiative. Of course, there is the remaining $280 million for a new crime analysis program, improvement of public safety communication technologies, and promotion of other high-tech crime-solving technologies.

Standing alone, the *Crime Identification Technology Act* would have been a tremendous victory for SEARCH and for the American people, but good things come in bunches, and so we also welcome the *National Crime Prevention and Privacy Compact* with open arms.[3]

I need not sing the compact's praises to this audience. With its passage, though, we can all look forward to a newly efficient and sensible interstate exchange of criminal history information for noncriminal justice purposes.

With the compact's help, the American people will have greater assurance that our school bus drivers, our child-care providers and our nursing home employees, to name just a few, are right for their jobs, right for our children and right for our parents.

As we move into the 21st century, information-sharing and technology are more than ever the bywords of law enforcement success. I would like to highlight a few areas where together we are making a difference.

As you know, on November 30, 1998, the National Instant Criminal Background Check System (NICS) replaced the interim system under the Brady Act. NICS has been a tremendous success.

Again, we look at technology as if it were something magical. To go to Clarksburg, West Virginia, to watch NICS in action, you are reminded all over again that technology will never work without people behind it; people who care, people who are well-trained to prepare for the challenges that those wonderful public servants dealt with as they began operating the system at the beginning of the Christmas season.

It was an extraordinary example of what we can do if we commit ourselves to making sure technology serves us, that we are its masters, and that we do not let it wrap us up and around its little finger. We are going to control it, or we are in trouble.

In the first 9 weeks of the NICS operation, the FBI denied more than 16,000 prospective gun transfers based on information provided by the system. States acting as "points of contact" denied many other sales. Also, a number of NICS denials resulted in the apprehension of wanted criminals who were seeking to purchase firearms. Simply stated, these denials and arrests translate into lives saved and less crime.

Of course, the criminal history records systems maintained by the states provide NICS with its backbone. And while the states have made great progress in improving their systems, there is more we can and must do, not only to strengthen NICS, but also to strengthen those systems that depend on state criminal history records.

The first summer job I had was in 1956. I worked at the Dade County, Florida, Sheriff's Office. There were three floors on the top of our old downtown courthouse. The crime laboratory was up there. The road patrol was up there. The jail was up there. I look at the differences between criminal information recording then and now and it staggers the imagination. Back then, all criminal histories were written on 3-inch by 5-inch cards!

We have come a long way. But even as I was leaving Dade County, I was still frustrated by the fact that criminal history records were incomplete in terms of dispositions. I knew there were people receiving bail and getting out of jail who probably would have been detained if their records had been complete.

The completion of these criminal history records is one of the keys to everything we are doing in law enforcement. We must continue that effort, and I would appreciate any suggestions you have as to what the Justice Department can do to promote that effort in every way possible.

[3] Title II of Pub. L. No. 105-251, the *National Criminal History Access and Child Protection Act*. The compact formalizes use of the Interstate Identification Index system for authorized noncriminal justice purposes.

One clear step is that every state needs to join the Interstate Identification Index (III). State participation in III will improve the quality, the accuracy and the timeliness of shared criminal history information.

I look forward to complete state participation in III by the year 2000. Again, let me know if you think of anything that we can do to improve this effort.

Since 1994, the Justice Department has distributed more than $250 million in grants for updating criminal history information. More is available. With your help, the NCHIP program has been a success, but we have much more to do.

One area on which we must focus and concentrate is providing security for the information we collect on computers. We are now engaged in an effort through the National Infrastructure Protection Center at the FBI to work with the private sector to develop the capacity to protect the precious information infrastructures that are oriented toward the cyberworld.

Today, our transportation, electrical, power, national defense and banking systems, and so many others, are tied into automation and into that critical infrastructure through cybertools. We are building tremendous databases. What would happen if a bad guy decides he is going to fuss with the information systems we develop instead of using guns or laundering money electronically? I do not think we have begun to consider how we protect those systems to ensure accuracy.

Ladies and gentlemen, if a 17-year-old hacker can break into sophisticated military networks, think of what he or she can do to some of our exposed information networks. We must continue to address this issue and keep one step ahead of the bad guys.

To achieve the desired security of these systems, we must consider this: As we build information systems and as we develop new technologies, we need to have the people who can operate and understand these systems. Today, we are not graduating enough people with literacy in computers and information technology. I would like to work with SEARCH to do everything we can to develop the capacity in state, local and federal governments to graduate people and to employ people with the skills necessary to take us into the next century with secure, effective, global information systems.

Information is such a prize. I tease OJP every now and then about the wonderful books they produce that I would receive while I was State Attorney in Miami. These books were stuffed with information. “Hey,” I would say, “this is great.” Then I would look and see that the book’s research was done 3 years before. By this time, the crack epidemic had hit Miami, and the picture was entirely different from that portrayed in the book. I did not understand what was going on.

Now, because of the work you are all doing, we are sharing information at every level — federal, regional, state and local — not just in the operation of the court system, but in the operation of what is happening in your community.

Is it a drug organization? Is it youth violence? Is it a major gang? Who is causing the problem? Getting that information, developing it, sharing it, and making it available to law enforcement throughout the region so that we can plan together is one of the most exciting opportunities that we have in law enforcement.

As we develop the information systems, we also have to develop procedures that allow law enforcement to collect appropriate information while not invading an individual’s privacy. This information will link regions and help prioritize crime initiatives in each community.

This is the dream I have for the Justice Department: that the U.S. Attorney will call together federal agencies to determine what they perceive to be the crime problems based on solid information developed through sound intelligence analysis. They will then meet with state and local agencies, agree on a plan to fight crime problems in the particular community, determine a response based not on the principles of turf or who gets credit, but on what is in the community’s best interest and what is consistent with the principles of federalism. Plans will then be made to implement what has been agreed upon.

We can make a difference if we use the information, the precious, current, accurate information that we are capable of collecting if we do it the right way. We are going to have opportunities from the patrol car to the jail to collect information and understand what is happening, to understand immediately who is coming out of prison. Ten years ago, I never dreamed this would happen.

You have made these opportunities happen for America. While some people believe that what you have done is not interesting or important, you have engaged in one of the most important undertakings in the criminal justice system — getting the right information and using it in a timely way to truly make a difference for the American people.

I go back to my challenge. We have an opportunity to dramatically impact the culture of violence in this nation. We cannot slow down. We have to move ahead with all the vigor that SEARCH has demonstrated over its 30 years.

Mr. Hawkins, you started something a long time ago, and an awful lot of people have been there along the way. Your work has been vitally important. It has made such a difference for this nation, and I, for one, think you are some of the heroes and heroines of the criminal justice system.

Thank you very much.

Question-and-answer Session

ATTORNEY GENERAL RENO: I have a question for you, and you may want to give me some answers. If you were the attorney general of the United States, what would you do to improve our efforts in support of your initiatives?

FIRST AUDIENCE MEMBER: What advice would you have for the media when they seek to explain the difference between the public expectation of applied criminal justice information and the current state of the uneven quality and completeness?

ATTORNEY GENERAL RENO: I would tell the media that we are in a state of transition. I would find your own examples similar to mine with the 3-inch by 5-inch index cards, and then show them the latest piece of justice information technology available in your jurisdiction. Tell the media that we are halfway between people who are age 45, 50 and 60 and just now becoming computer literate and the 17-year-olds who can run technological circles around them.

We are in a state of transition. We are going to look back on law enforcement 20 years from now and say we were able to accomplish all this with as little as we had. I think you explain it in those terms and they understand better.

One of the things I have tried to accomplish in these last 6 years is to not let partisan politics influence decisions on crime and criminal justice. Republicans do not like crime and Democrats do not like crime. I came from a jurisdiction where there was total bipartisanship, and oftentimes total nonpartisanship. I have been in San Diego, California, with a Republican sheriff, a Republican mayor and the president of the United States, and everybody is standing there talking about what we were doing together to address the issue of crime.

I think that for too long, public officials and policy-setters thought the way you handle crime was to build more jails and add more police. Forget about judges or prosecutors, and certainly do not add public defenders, although you have to convince people that the public defender is an essential part of the whole criminal justice system, and you have to look at the system as a whole.

It was not popular to add technology and make the system more effective, or even to update criminal history records manually.

I think we have helped, all of us working together have helped the American people understand that if we can get current information in the most accurate form possible, we are going to make the criminal justice system work better.

FIRST AUDIENCE MEMBER: I gave the reporter your quote from the 1996 symposium that “information is the lifeblood of the criminal justice system.” He started saying that it was a contaminated system. I think it is more accurate to compare the system to a blood bank where the level varies, and we are trying to recruit more donors.

ATTORNEY GENERAL RENO: Perfect.

SECOND AUDIENCE MEMBER: I did not think I would be in this position this morning, but I want to thank you for your efforts with the Community-Oriented Policing Services (COPS) program, especially from the Commonwealth of Virginia. It has been tremendous to have neighborhood enforcement officers walking the streets and walking the beats.

I work for the probation and parole side of the house, and we have always been walking the streets and walking the beats. What has evolved is a new partnership between probation and parole and neighborhood officers. Communication between law enforcement officers looking for offenders and probation and parole personnel who know where the offenders are has greatly improved.

One effort I would like to see the Justice Department consider is an information system that includes probation and parole officers, because we visit these people, we are in their homes, we know where they are. Do you have any comments regarding that effort?

ATTORNEY GENERAL RENO: First, it is so exciting to see the partnerships developing between probation and police officers. They are riding together in a number of jurisdictions.

It seems to me we have to do two things, and we are engaged in doing two things in the Justice Department. First, when you say communicate together, you mean that the law enforcement officer and the probation officer are verbally communicating together while in a squad car or on the streets as they travel to the home of a probationer who is supposed to be home but who is not.

As for communicating electronically, with narrow banding because of the sell-off of spectrum space, local law enforcement, corrections and the like are going to have to do so much to prepare both for the narrow banding and for the wireless communication systems. It is going to cost many jurisdictions a lot of money. We are going to have to figure out how to do it in the wisest way possible and we are engaged in that.

Second, let me explore when I get back to the Justice Department just what we are doing in terms of probation and COPS, because I think that is an excellent idea.

The other important point is that it is not just about law enforcement. When a probation officer knocks on a juvenile offender's door at 10:05 p.m. when he is due in at 10 p.m. to comply with his curfew, and the police officer accompanies the probation officer, we find in a number of jurisdictions that the officer is getting to know the kid, he is responding to the juvenile, and the officer is becoming the juvenile's mentor.

SECOND AUDIENCE MEMBER: I am talking about the adult probation side, but what also happened is that we have been able to notify officers that they are serving warrants to very violent offenders They have been able to proceed with arrests more safely, and they have been able to accompany us into neighbor–hoods where we need some assistance from law enforcement. So it has been a wonderful experience. We are now verbally communicating as opposed to doing it through an automation process.

ATTORNEY GENERAL RENO: I alluded to it during my remarks. If we are able to check for offenders coming out of prison, you look at a recidivist and you can see a crime waiting to happen. If the probation officer or the parole officer is accompanied by the police officer in that community setting when he or she makes a call, they can …

SECOND AUDIENCE MEMBER: There is a lot that could be done. We can get them on technical violations as opposed to violations of law.

ATTORNEY GENERAL RENO: Let me go back to one other point with respect to community policing. We are seeing the development of community justice systems, sometimes in urban areas, and sometimes in more suburban areas. How they exchange information in that community setting is also extremely important.

THIRD AUDIENCE MEMBER: As private companies that operate correctional facilities move toward operating first-line jails, could you address their ability as private citizens to access III and the National Crime Information Center?

ATTORNEY GENERAL RENO: Let me make sure that I get your name and address. I frankly have not considered that. I would like to investigate and inform myself more completely on it and get back to you if I may. I will take one more question.

FOURTH AUDIENCE MEMBER: If you were to look deep into your wise crystal ball, do you ever foresee a national identification card being given out, as well as a national password to protect any of our information?

ATTORNEY GENERAL RENO: I do not think so. I think that the whole issue with respect to privacy is one of the great issues that we are going to have to grapple with, not just in the context of what we are working on here today, but in terms of what the Internet provides — the wonderful opportunities and the extraordinary challenges. It is a possibility. I do not know the answer. My crystal ball gets dim.

Thank you all. I am very glad I could be here, and I look forward to seeing you all again soon.

Keynote Address

By United States Senator Mike DeWine

R-Ohio

Sen. Mike DeWine was sworn in to the United States Senate on January 4, 1995, as the first Republican Senator to represent the Buckeye State in more than two decades.

Sen. DeWine holds seats on the Senate Judiciary, Labor and Human Resources and Select Intelligence committees. In addition, he is Chair of the Senate Subcommittee on Antitrust, Business Rights and Competition of the Judiciary Committee and the Senate Subcommittee on Employment and Training of the Labor and Human Resources Committee.

Since his arrival in the Senate, Sen. DeWine has worked to advance technology for local law enforcement officials, improve the lives of at-risk children, promote the health and safety of babies and new mothers, balance the federal budget and reform the nation's welfare and health care systems.

After earning degrees from Miami University, Ohio, in 1969, and from Ohio Northern University Law School in 1972, Sen. DeWine became Assistant Prosecuting Attorney for Greene County, Ohio. In 1976, he was elected Greene County Prosecuting Attorney. Sen. DeWine was elected to the Ohio State Senate in 1980 and then to the U.S. House of Representatives in 1982. During his tenure in the Ohio Senate, Sen. DeWine was instrumental in the passage of a strict drunk driving law, and in the U.S. House, he led passage of landmark federal legislation to protect children victimized by violent crime.

In January 1991, Sen. DeWine was sworn in as Ohio's 59th Lieutenant Governor.

Let me begin by thanking SEARCH, The National Consortium for Justice Information and Statistics, and the Bureau of Justice Assistance (BJA), U.S. Department of Justice, for bringing together this most important symposium.

I would also like to take a moment to salute SEARCH, which is celebrating its 30th Anniversary. Three decades ago, SEARCH took a leadership role in developing the interstate capability to electronically exchange criminal history records. Since this successful effort, SEARCH has matured into a multifaceted organization representing the collective voice of states on national information management issues. All Americans have benefited from SEARCH's dedication to improving the criminal justice system through the intelligent application of technology. SEARCH has made America's neighborhoods safer. Thank you.

I have been asked to speak today on the subject of anti-crime technology and the issue of integration. This is a particularly timely topic for me, because of the recent enactment of my legislation called the *Crime Identification Technology Act of 1998* (CITA).[1] This new law gives us all an even greater opportunity to realize the objectives that will be addressed by this symposium.

While reviewing my remarks, I was reminded of a story of what can happen when email messages go astray. Consider the case of an Ohio man who left the snow-filled streets of Cleveland for a vacation in Florida. His wife was planning to meet him there the next day. When the man reached his hotel, he decided to send his wife a quick email. Unable to find the scrap of paper on which he had written her email address, he did his best to type it from memory. Unfortunately, he missed one letter, and his note was directed instead to an elderly preacher's wife whose husband had passed away only the day before. When the grieving widow checked her email, she took one look at the monitor, let out a piercing scream, and fell to the floor in a dead faint. At the sound, her family rushed into the room and saw this note on the screen: "Dearest Wife: Just got checked in. Everything prepared for your arrival tomorrow. P.S. Sure is hot down here."

If there is one thing that more than 25 years of experience working in the criminal justice system has taught me, it is that information is absolutely crucial to successful law enforcement. As a prosecutor in Greene County, Ohio; as lieutenant governor overseeing Ohio's anti-crime and anti-drug efforts; and as a member of first the House and now the Senate judiciary committees, I have learned that the decisions we make in law

[1] Pub. L. No. 105-251 (1998).

enforcement are only as good as the information we have available.

My belief in the importance of anti-crime technology has led me to work on several initiatives over the years. All have now become law, and they are up and running. I am talking about the 5-percent set-aside for criminal history improvement from the Byrne grant program[2]; the State Identification System Program under the 1996 Antiterrorism bill; and my yearly support for appropriations for the DNA improvement program, the Regional Information Sharing System program, and other programs to support the development and modernization of anti-crime technology at all levels of government.

I must confess that, through my work on these programs, I have learned something about the need for integration: We need to do more. Two fundamental factors have converged in recent years to make the integration of criminal justice systems even more important as we face a new millennium.

First, revolutionary improvements in information and identification technologies have created opportunities, indeed responsibilities, for all our nation's criminal justice agencies to build integrated information, identification and communications systems. We now have the necessary tools to build the kinds of systems and linkages between systems that are so desperately needed to allow our justice agencies to realize their full potential. Technology continues to be a powerful tool in the arsenal of weapons available to justice agencies in their fight against crime.

Second, the business of law enforcement is changing in fundamental respects as a consequence of the availability and power of new and emerging technologies, but also because of the growing demand for information by other agencies and by the general public, along with a demand for greater accountability.

With rapid advances in technology, justice agencies are able to capture, collect, transmit and analyze an expanding array of information — such as photographs, maps, fingerprints and investigative records — with extraordinary speed and flexibility. Justice agencies increasingly recognize the inherent value and power of the community within which they operate, and contemporary trends in community-based policing, community-based courts and community corrections leverage local resources to better respond to crime and its social roots.

Law enforcement agencies have adopted sophisticated crime-mapping and forecasting technologies to proactively target crime at its source. By sharing information and decisionmaking with other city and county agencies, as well as with the community at large in new and innovative ways, they are able to marshal vast resources in their efforts to combat crime. These programs and the technologies that support them certainly share some of the credit for the significant reductions in crime we have witnessed across the nation.

One of my major purposes in sponsoring CITA last year was to achieve integration in its broadest sense. Of course, CITA provides for system integration, permitting all criminal justice components to share information and communicate more effectively and on a real-time basis. There is also, however, a tremendous need to integrate the patchwork of federal programs that fund anti-crime technology.

If we continue this mandated, discrete approach, there will never be enough money, or integration. In this connection, the intent of CITA is to provide a dedicated, integrated stream of funding to help states establish and upgrade their anti-crime technology, while providing accountability and efficiency to a disparate government-funding matrix.

You may be aware that the model for CITA was the National Criminal History Improvement Program (NCHIP), which is an excellent example of how state crime technology needs can be met, and limited federal resources maximized, through an integrated federal-state approach.

CITA attempts to address virtually every technology-based information, identification and forensic need of state and local criminal justice agencies. In addition, we wanted to make sure that states had the resources to participate in our national information and identification systems, namely, the Interstate

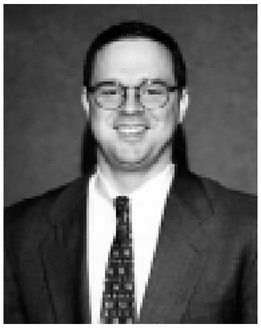
[2] Through the Edward Byrne Memorial State and Local Law Enforcement Assistance Program, BJA provides formula grants for activities related to crime and violence prevention and control, including funding for educational and training programs, technical assistance, and national or multijurisdictional projects and demonstration programs that are likely to be successful in more than one jurisdiction.

Identification Index and the *National Crime Prevention and Privacy Compact*, the Integrated Automated Fingerprint Identification System, the National Crime Information Center 2000, the Combined DNA Index System, and the National Integrated Ballistics Network.

A foundation is also laid in CITA for the compact, which establishes a uniform standard for the interstate and federal-state exchange of criminal history records for certain public safety purposes. Clearly, this is a wonderful example of SEARCH's vision of integration and the public's demand for protection that have converged to create this law.

As you know, CITA authorizes $250 million a year over 5 years for anti-crime technology grants for states and local governments. However, the President's budget earmarks only $50 million for Fiscal Year 2000 to support CITA. I think this is a huge mistake. This act has terrific potential to integrate anti-crime technology and improve crimefighting at the federal, state and local levels. CITA deserves full funding.

I would like to ask you to work with me to let your members of Congress know how important this law is to you, and the difference it would make in your communities if it were fully funded. If we do this, together we will make a difference in every neighborhood in this country. Thank you, and have a wonderful symposium.



Paul F. Kendall, General Counsel for the Office of Justice Programs (OJP), U.S. Department of Justice, is the Executive Chairman of OJP's Information Technology Executive Council, as well as Chairman of the Executive Council's Inter-Governmental Information Sharing Working Group, the Intelligence Systems Policy Review Board, and the Privacy Task Force.

Mr. Kendall is leading a variety of efforts in developing state and local coordinated information technology programs, and is leading the Intelligence Systems Policy Review Board's examination of legal and public policy issues associated with information-sharing.

Prior to his arrival at OJP, Mr. Kendall held positions of Senior Counsel at the Federal Mines Safety Board, and Assistant General Counsel of the Legal Services Corporation, as well as other positions in public and private practice.

Mr. Kendall received his Bachelor of Arts degree from Columbia College of Columbia University, his Master in Business Administration from the University of Maryland, and his Juris Doctor from The Catholic University of America, Columbus School of Law.

Improved Criminal Justice Through Information-Sharing: Office of Justice Programs' Justice Integration Initiative

By Paul F. Kendall
General Counsel, Office of Justice Programs[1]
U.S. Department of Justice

There is no doubt that information and communications technology has changed the face of criminal justice. Increased criminal sophistication and mobility require criminal justice components to implement improved information-sharing systems capable of interagency and multijurisdictional communication. In response to the expanded information needs of the law enforcement and criminal justice communities, many states and localities are developing plans to efficiently share accurate information through integrated criminal justice information architectures.

Integrated architectures encompass the ability and desire of criminal justice agencies to share information within their organizations and between their organizations and other criminal justice components. Recent information technology advances have made integration possible for large and small agencies alike. New technological possibilities, in conjunction with state and local leadership and support from the federal government, are breaking the traditional information-sharing barriers that separate criminal justice agencies and are moving us toward a more fully integrated justice system.

The Office of Justice Programs (OJP) and its five bureaus — the National Institute of Justice, the Bureau of Justice Statistics, the Bureau of Justice Assistance, the Office of Juvenile Justice and Delinquency Prevention, and the Office for Victims of Crime — assist state and local governments through grant programs designed to foster partnerships to improve criminal justice and juvenile justice systems nationwide. As part of this mission, OJP and its bureaus recognize the need to assist state and local governments in developing information-sharing capabilities.

OJP envisions a nationwide information system capability for improved criminal justice information-sharing that provides state and local stakeholders responsible for law enforcement, courts, prosecution, public defense, corrections, probation and parole with immediate access to all the information they need to respond to and resolve the consequences of criminal activity. OJP foresees this nationwide-access capability being accomplished through

[1] Mr. Kendall is leading OJP's integrated information technology initiative.

information architectures that facilitate the interoperability of locally autonomous criminal justice information-sharing systems.

This vision of improved criminal justice information-sharing is tied inextricably to the development of intergovernmental sharing capabilities that allow seamless information transfers between all governmental agencies, including education, health and welfare, transportation and social services. OJP is working to expand the concept of criminal justice information architectures so these architectures can operate within larger intergovernmental designs to exchange necessary and appropriate information among and between all governmental agencies.

In the Fall of 1997, OJP recognized that it could achieve its vision through the efficient, coordinated and targeted use of grant funds and technical assistance resources to help state and local governments create integrated information architectures for their criminal justice systems. In 1998, OJP undertook a field-outreach initiative to gain insight into current state and local justice integration initiatives, and to elicit ideas from state and local criminal justice leaders as to how OJP — in its federal role — could best assist them in reaching their information technology goals. Based on this field input, OJP has defined its federal role in support of integrated justice, and has designed and implemented a number of actions to facilitate and assist integration efforts at the state and local levels.

OJP's Federal Role in Support of Integrated Justice

There are many integration efforts underway throughout the country, both in state and local jurisdictions and at a variety of criminal justice and technology organizations and associations. The key to creating truly national information-sharing and integration capabilities is to harness the efforts of these valuable campaigns and provide coordination and communication mechanisms under which each effort can learn from and build upon the others' successes. The federal government has the ability to organize and bring together these nationwide integration efforts. It is critical that the federal government act as a facilitator to coordinate promising state and local initiatives, and not seek to achieve national information capabilities through top-down technology or planning requirements.

Due to its rich history of state and local criminal justice assistance, OJP is the federal agency that is uniquely positioned to provide leadership and funding support — as well as to facilitate consensus building and coordination — to assist state and local technology initiatives. For example, OJP possesses clear statutory authority to encourage state and local integration through grants for technical assistance and training. In addition to providing grants to state and local governments, OJP has criminal justice resources that enable it to provide forums to research and evaluate ongoing integration efforts throughout the country while facilitating and encouraging dialogue among criminal justice agencies. Moreover, OJP, with its statutorily supported tradition of promoting and assisting criminal justice, has developed a full range of expertise in state and local criminal justice issues.

The OJP Integration Initiative is harnessing the unique resources of the office, its bureaus and its many technical assistance providers to propel forward the coordination of state and local justice integration efforts. Just as the federal government is tasked with coordinating national integration efforts, OJP must coordinate its own programmatic resources and those of its various technical assistance providers that work with state and local governments on integrated technology projects.

OJP has worked throughout 1998 to develop an internal coordination strategy, as well as a technical assistance and funding strategy, for the field. The result is the 1999 Integration Initiative Action Plan. The 1999 action plan includes OJP's coordination strategies and eight specific projects to support state and local justice integration as recommended by the field. These projects are being implemented by targeting the expertise of criminal justice organizations and technical assistance providers, such as SEARCH, that bring a wealth of knowledge to the initiative.

1999 Action Plan: OJP Action Items

1. Implementing a Funding Strategy

The first 1999 action item is the implementation of a funding and award-guidance strategy to promote the efficient and coordinated deployment of information technology funding from OJP and its bureaus. The generalized basis for OJP's funding strategy is found in more than 40 of its bureaus' statutory provisions which contain expressed or implied language authorizing information technology purchases. Each of these statutes provides for and encourages the development of information-sharing systems to further the fight against crime. OJP views the coordination of these statutes to provide necessary planning, training and technical assistance grants as key to enabling state and local governments to implement technologies that are interoperable within, as well as outside, individual state, local, regional and federal information systems and networks.

Additionally, the field recommended that OJP use its funding authority to promote and encourage communication and coordination between state and local jurisdictions. To this end, OJP is implementing an award-guidance strategy that requires information technology funding recipients to advise points of contact in their states that they are undertaking information technology projects. This guidance strategy is designed to ensure that state agencies and local jurisdictions receiving federal information technology funding are in communication with the bodies responsible for statewide justice integration initiatives, and can use their resources to build interoperable, rather than isolated, systems.

2. Developing a "Business Case" for Integration

The second action item is the development of a "business case" for integration. There is a need to develop an education and marketing tool to explain to executives, legislators, the judiciary and the public the necessity and benefits of integrated justice. The field refers to this tool as the "Business Case for Integration." The business case will highlight integration's ability to improve justice system fairness, efficiency and economy toward the ultimate goal of increased public safety. Once developed, OJP can use the business case to assist state and local criminal justice leaders in garnering funding and legislative support by presenting their initiatives to high-level officials in their jurisdictions.

3. Study Governance Structures

The third action item is a study of state and local integrated information technology governance structures. In this project, a survey of all states will be conducted to ascertain the type, quality and capability of governance processes and structures in use or contemplated nationwide. Similar surveys will be conducted at the local level, including a review of how local governance structures relate to state-level structures. Following the surveys, the findings will be analyzed to evaluate the quality and effectiveness of the approach taken by each state or jurisdiction, highlighting the strengths and weaknesses of the various governance approaches. Study results will be used by the field to improve upon their existing governance structures and, where no structures are yet in place, to serve as possible models of successful methods.

4. Discuss Integration Standards

The fourth action item is the initiation of a national discussion on integration standards. There is a consensus within the criminal justice community that standards are key to the successful integration of criminal justice information systems. The field has recommended that OJP coordinate the activities of criminal justice standards-setting bodies to develop a national consensus on technical and data integration standards. In addition, the field recommended that OJP conduct research to identify existing standards and "gaps" that might exist. In its federal role, OJP can assist in coordinating and facilitating the participation of all criminal justice standards-setting organizations in a national standards-setting initiative.

5. Review State, Local Legislation

The fifth action item is a state and local legislative review. The field requested an inventory of legislation supporting integration initiatives and governance structures to assist jurisdictions in drafting similar provisions or amending outdated legislation. This project proposes to inventory existing legislation passed or being contemplated by state and local governments aimed at integration governance, planning and interoperability. In addition, existing legislation will be analyzed, and information on best practices supporting integration will be made available to state and local governments.

6. Study Information Exchange

The sixth action item is a study to identify how information moves within the criminal justice system, and where information exchange points exist between criminal justice agencies. The field recommended this type of study to develop an information exchange model for criminal justice integration. This project proposes to study the types of information being exchanged by criminal justice components, determine the types that should be exchanged, and review the implications of standards, coordination, governance, and other facets of information exchange.

7. Improve Procurement Strategies

The seventh action item involves the development of a strategy to improve procurement processes — including Requests for Proposals (RFPs) — for information technology initiatives. The field recommended that OJP work with legislatures and the private sector to rethink the procurement process. This project proposes to compile information about successful RFP strategies and highlight these practices in briefings to governors and — working through the National Conference of State Legislators — state legislators. These briefings will illustrate how outdated procurement processes impede integration and interoperability, and suggest the need for legislation to improve the procurement area.

8. Develop National Web-based Resource

The final action item is, perhaps, the most important example of how OJP as a federal agency can assist and support state- and local-level integrated justice initiatives.

The eighth action item involves the design, development and implementation of a National Integration Resource, which will be a dynamic Web-based resource enabling criminal justice components at all government levels to access and obtain timely and useful information on integration processes, initiatives and new developments. The field recommended a "people-oriented" resource center that provides analytical, knowledgeable and up-to-date information, as well as on-line technical assistance and integration "help-desk" services.

The National Integration Resource Center will collect and make available the findings and related information from each action item described above, as well as a wealth of other information, such as:

- state integration profiles, best-practices compilations and success stories,
- funding approaches used by various states,
- lessons learned pursuing integration and interoperability,
- system descriptions and overviews,
- telecommunications approaches,
- mobile data terminal and wireless initiatives, and
- model integrated systems.

In addition, the resource center will provide on-line communication capabilities such as conferencing and newsgroups, allowing criminal justice personnel to discuss ongoing integration activities over a secure, yet open and easily accessible, medium.

Integration Initiative: Expanding the Scope

OJP recognizes that "integrated government" is the wave of the future. In facilitating integrated criminal justice, we must be mindful not to create a justice system that cannot interoperate with other public safety agencies and affiliated government agencies, such as education, health services, social services and transportation. Many state and local governments are engaging in information architecture planning that includes all government services, and it is crucial that OJP support this broad view of integration.

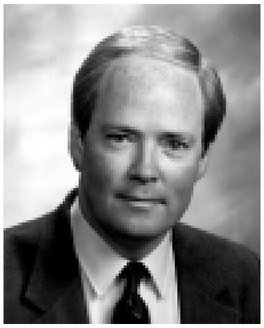
OJP is engaging in a number of activities that support the broad concept of integrated government and the development of criminal justice architectures within larger state architectural plans.

For example, the Bureau of Justice Assistance awarded a grant to the National Association of State Information Resource Executives (NASIRE) in 1998 to conduct a State Information System Architecture Survey. Through NASIRE, OJP is surveying state-level chief information officers to determine the status of initiatives to develop strategic plans and information architectures, and to elevate the importance of the criminal justice system in their planning agendas.

In addition, OJP has entered into an Interagency Agreement with the National Science Foundation (NSF) to join the Federal Web Consortium. This agreement allows OJP to attend Federal Web Consortium symposia, exchange ideas with other federal agencies about the future of technology, learn about research being conducted that might affect our plans, identify research needed to assist OJP in improving criminal justice community support, and partner with NSF and other research agencies to pursue mutually beneficial projects. OJP joined the Federal Web Consortium after the field urged the office to build relationships with other federal agencies to facilitate coordination of information technology research, funding and planning at the federal level. Membership in the Federal Web Consortium allows OJP to familiarize itself with the research community, and to inform and excite the consortium about developing new technologies with criminal justice applications.

Vision for the Future: OJP's Ongoing Federal Role

OJP's success in promoting integrated criminal justice is a direct result of the enthusiasm and dedication of hundreds of state and local criminal justice leaders throughout the country. OJP is committed to continuing its bottom-up approach, where state and local stakeholders have direct impact on funding, technical assistance strategies and infrastructure development employed by the office. It is the agency's goal to develop the National Integration Resource Center as a mechanism whereby state and local practitioners can inform OJP about what works in the field and where assistance is most needed. OJP will continue to target its resources based on field input, and will continue to make available to the field the knowledge and expertise of criminal justice technical assistance providers. Through providing leadership, coordination and support at the federal level, OJP hopes to achieve a nationwide criminal justice information-sharing capability.



David J. Roberts has served as Deputy Executive Director of SEARCH's Research & Technology Division since 1987. Mr. Roberts provides technical assistance to justice agencies throughout the nation, addressing such issues as automation planning, integration of information systems and the strategic use of information.

Mr. Roberts directed the 1999 Symposium on Integrated Justice Information Systems, the 1997 National Conference on Justice Agencies and the Internet (cosponsored by SEARCH and DOJ's Bureau of Justice Statistics), and the 1994 International Symposium on Criminal Justice Information Systems and Technology and the 1996 Symposium on Integrated Criminal Justice Information Systems (both sponsored by the Bureau of Justice Assistance).

In addition, Mr. Roberts has served as Staff Director of the joint BJS/FBI project on NIBRS implementation among law enforcement agencies, for which he authored the project report Implementing the National Incident-Based Reporting Systems: A Project Status Report.

Mr. Roberts holds an M.A. from the School of Criminal Justice, State University of New York at Albany; a Master of Criminal Justice Administration from Oklahoma City University; and a B.S. in Law Enforcement and Criminology from Metropolitan State College, Denver, Colorado.

Integrated Justice Information Systems Planning and Implementation: Organizing for Change

By David J. Roberts
Deputy Executive Director
SEARCH, The National Consortium for Justice Information and Statistics

Introduction

Justice agencies throughout the nation increasingly recognize the importance of integrating their information systems in order to share critical data, documents, images and key transactions. The need to electronically share accurate and complete information in a timely, secure and efficient manner is driven by the operational requirements of agencies at the local, state and federal levels, as well as a host of state and federal legislative mandates that have been enacted in recent years.[1] In recognition of this need to share critical data, state and local jurisdictions are actively developing plans and programs for comprehensive integrated justice information systems.

Integrated systems improve the quality of information, and thereby the quality of decisions, by eliminating error-prone redundant data entry. In addition, by sharing data between systems, integration typically improves the timely access to information — a critical factor at many criminal justice decision points (for example, setting bail). Moreover, integration enables the sharing of crucial information without regard to time or space; multiple users can access the same record simultaneously from remote locations around the clock.

Successful integration of information systems requires careful planning and effective organization. Jurisdictions must articulate a vision, define the scope and objectives of their project, establish an effective organizational structure, recruit initiative sponsors, secure funding, develop comprehensive and detailed strategic plans, and address a host of technical and policy issues to enable the sharing of information within and between agencies. This paper will address fundamental issues associated with integrated systems planning and implementation at the local, regional and state levels.

[1] *See*, for example, the National Child Protection Act of 1993, Pub. L. 103-159, codified in 42 U.S.C. §§ 5119 et seq.; The Brady Handgun Violence Prevention Act, Pub. L. 103-159, 107 Stat. 1536, as codified in 18 U.S.C. § 922; The Lautenberg Amendment, Pub. L. 104-208 (contained in the 1997 Omnibus Appropriations Act), codified as 18 U.S.C. § 922(g); INS Alien Conviction Notification, 42 U.S.C. § 3753(a)(11); Jacob Wetterling Crimes Against Children and Sexually Violent Offender Registration Act (including Megan's Law), Pub. L. 103-322, § 170101, codified as 42 U.S.C. § 14071; and National Protection Order File, Pub. L. 104-236, codified as 42 U.S.C. § 14072.

Defining Integration

It should be acknowledged that "integrated justice information systems" means different things to different people in different contexts. Law enforcement agencies need to share information between divisions within their own department (for example, patrol, crime analysis, detectives, etc.), as well as with other law enforcement agencies in the region, state and nation. Prosecuting attorneys need much of the same information already captured by the police in order to make informed charging decisions. In turn, this same information is needed by the local court, jail, public defender and pretrial services office. Additionally, each of these agencies makes decisions regarding the persons/cases involved, the consequences of which should be shared with others. In fact, these decisions may trigger actions by other agencies and/or jurisdictions (for example, scheduling an appearance in court, filing a motion, initiating a pre-sentence investigation, etc.) which, in turn, are recorded in individually identifiable longitudinal files known as criminal history records.

Integration encompasses a variety of functions designed to enable the timely and efficient sharing of information[2] within and between agencies. *Within* agencies, the primary objective of integration is to eliminate duplicate data entry, enable access to information that is not otherwise available, and ensure the timely sharing of critical data. Often, systems have been developed in isolation of one another or on incompatible technologies, resulting in independent systems that may share many common data concepts, but that cannot communicate. Duplicate data entry hinders agency operations, consumes precious resources, retards timely access and undermines data quality. Additionally, however, agencies seek to achieve new synergies by integrating, collating and combining information in new and innovative ways. Police departments, for example, are better able to target crime and intervene proactively when their dispatch, records management, detective case management and crime analysis systems share on-line information that is immediately and broadly accessible.

Beyond improving the internal operations of justice agencies, integration is more expansively viewed as enabling the sharing of critical information *between* agencies. Integration efforts are often referred to as *horizontal* (for example, among different divisions of the same court system, or between the local police department, prosecutor and court) or *vertical* (for example, from limited to general jurisdiction courts, from trial to appellate and state supreme courts, and from local agencies to state and national/federal systems).[3]

Functional Components of Integration

Interagency integration, whether horizontal or vertical, generally refers to the ability to access and share critical information at key decision points throughout the justice process. The functions we normally consider in integration efforts between agencies include the ability to:

1. Automatically *query* local, regional, statewide and national databases to assess the criminal justice status of a person (for example, determining whether a person is currently wanted by another jurisdiction, has charges pending in another jurisdiction, is currently under some form of correctional supervision, or has a criminal history at the state or national level);
2. Automatically *push* information to another agency, based on actions taken within the originating agency (for example, reporting of arrest information, together with supporting fingerprints and mugshot, to the state and national criminal history repositories based on new information in the local database; when a law enforcement agency makes an arrest and enters this information in its records management system, it should "push" information to the prosecuting attorney's office for use in the prosecutor case intake process);

[2] The term "information" is used here in its broadest sense to incorporate data, images (photograph, document and fingerprint), case records, calendar events and electronic messages.

[3] SEARCH, "National Task Force Report on Court Automation and Integration" (unpublished report, 1998) page 3.

3. Automatically *pull* information from other systems for incorporation into the recipient agency system (for example, populating a correctional information system with offender information captured in the pre-sentence investigation, together with court sentencing information);

4. *Publish* information regarding people, cases, events and agency actions (for example, both electronic and paper publishing of information regarding scheduled court events, crime mapping, availability of community resources, criminal history records, sex offender registries, etc.); and

5. *Subscribe to a notification service* (for example, probation agencies and perhaps individual probation officers should be able to formally subscribe to a notification service that will enable them to be automatically notified whenever one of their clients is arrested or otherwise involved in the justice system, as should prosecutors with cases pending against a defendant, judges who have suspended sentencing or otherwise suspended proceedings regarding a defendant, and other actors in the justice process).

Justice agencies throughout the nation already share considerable information. It is important to recognize that regional, statewide and national systems currently exist to facilitate access to and sharing of key information among many of the actors in the justice enterprise. In addition, some of the information exchange contemplated in these five basic functions is currently accomplished with existing technology or is being developed in new systems, but much is also still done by hand through the ceaseless efforts of dedicated local practitioners. Integration efforts are designed to automate many of these operations, reengineer systems and processes, and achieve new capabilities with greater efficiency and effectiveness.

Foundation Principles of Integration

There are several principles that should be incorporated into the overall integration effort:

1. Data should be captured at the originating point, rather than trying to reconstruct it down line or have others capture it;

2. Data should be captured once and used many times, leveraging existing resources and improving data quality;

3. The integrated system should be driven by the operational systems of participating agencies, not separate from the systems supporting the agencies; and

4. The capabilities for generalized automatic query, push, pull, publish and subscription should be constructed as general capabilities of the system, so that, for example, additional automatic reporting can easily be implemented as additional requirements are identified.

Interagency Information Exchange

It is important to recognize that building integrated justice information systems does not mean that *all* information between agencies is shared, without regard to the event, the agencies involved or the sensitivity of the information available. Agencies need to share key information at critical decision points throughout the justice process.

At arrest, for example, the arresting agency typically transmits certain information regarding the arrestee to the state criminal history records repository (for example, name, age, sex, race, driver's license number, electronic image of the arrestee's fingerprints, etc.) to record the arrest transaction in the instant case, but also to verify the arrested person's identity and determine whether the arrestee has a criminal history record in the resident state, or in other jurisdictions around the nation. In addition, the local agency will also query other state and national systems to determine whether there are any outstanding warrants, detainers, or other holds on the arrestee. For these transactions, the local arresting agency does not need to share *all* information regarding the arrestee or the event which led to the arrest, but only that information necessary for the discrete transaction check for "outstanding warrants" or "verify identity and report arrest transaction to the criminal history repository." These same transactions are completed by law enforcement agencies throughout the nation whenever they secure an arrest.

These transactions, and many other routine information exchanges and queries, might be characterized as *conversations*, that is, discrete exchanges of information between two or more agencies (or units within a single agency). These conversations occur at regular events (for example, at arrest, charging, initial appearance, trial, adjudication, disposition, etc.) and the transactions are remarkably consistent in justice agencies throughout the nation.

Some of the conversations are very terse: "Here is information you need," followed by "Thank you, I have successfully received your information." Other conversations affect the receiver system more directly: "Here is a question I want to ask you," followed by "Here is the answer you requested." Some conversations affect the recipient's database: "Here is a disposition report to append to your history record," followed by "Thank you, I have done so." Some conversations can be complex: "Based on the enclosed identification data, search your master index and if you find a match, tell the other systems holding data on this person to send it to me," followed by "I have carried out your request and you can expect data from the systems named here."

Many of the primary events that trigger conversations between agencies in the criminal justice process were generally identified in the excellent schematic of the criminal justice process created in 1967 for the President's Commission on Law Enforcement and Administration of Justice,[4] recently updated by the Bureau of Justice Statistics.[5] From this historical research, and from the ongoing work of several jurisdictions in integrated systems implementation, we know many of the key events that trigger the conversations, the agencies involved, and the general nature and content of information exchanged in the conversations. It is important to note, however, that this schematic represents the general life cycle of criminal justice *case processing*, not the systematic processing of information throughout the entirety of the justice enterprise.

Documenting the key information transaction points and the conversations that occur at each of these events (that is, creating an accurate model of the justice information system processing, which includes identifying common events that trigger conversations, the agencies involved, and the nature and content of these conversations) will greatly facilitate integrated systems planning and design. SEARCH is working closely with the Bureau of Justice Assistance and the Office of Justice Programs in undertaking a project to complete this important research and, in doing so, to lay the foundation for integrated systems planning and implementation at the local, regional, state and federal levels.

Understanding Local, State and Federal Responsibilities

It is important to differentiate responsibilities at the local, state and federal levels regarding integrated systems planning, implementation and support. Local justice agencies are responsible for acquiring, creating and maintaining information systems that meet their internal operational needs. In addition, they have an interest and responsibility to share information with other agencies within and outside their immediate jurisdiction, and a continuing need to access and report information to regional, statewide and national systems.

The state has responsibility for creating a statewide infrastructure that will enable agencies to share information with other local jurisdictions throughout the state in a common format, and to share information with statewide systems. In this way, local agencies will have access to statewide systems, and the ability to share information with other states and localities. The state, therefore, is largely responsible for building the infrastructure necessary to support horizontal integration initiatives, and has primary responsibility for creating, adopting and maintaining state information systems and serving as the gateway to national and federal systems.[6] It should not be the state's responsibility to ensure that local justice agencies

[4] President's Commission on Law Enforcement and Administration of Justice, *The Challenge of Crime in a Free Society* (Washington, D.C.: Government Printing Office, 1967).

[5] *See* revised schematic at http://www.ojp.usdoj.gov/bjs/flowchart.htm

[6] It should be noted, however, that in some jurisdictions, the state has opted to create and maintain information systems that meet the operational needs of local users as a method of enabling integration. This distributed approach means that the state has assumed a significant data processing support strategy.

electronically share person, event, case or process data within the local unit of government.

In a similar vein, the federal responsibility is primarily for building and maintaining the national information infrastructure necessary to enable sharing of key information between states, to serve as a gateway for state and local agencies to various national and federal information systems, and to work with state and local jurisdictions to create, support and maintain new and emerging systems with national/interstate jurisdiction, such as the Integrated Automated Fingerprint Identification System (IAFIS), the Combined DNA Index System (CODIS) and the National Crime Information Center (NCIC) programs. Additionally, it is a legitimate federal responsibility to ensure that national and federal systems are integrated, non-redundant and responsive to the needs of state and local users.

The federal government also has responsibility to serve as a gateway to selected international systems. These objectives are accomplished through collaborative work with state and local agencies in the development and adoption of standards, the building of national and federal systems, and support in assisting local agencies in upgrading their general information technology capabilities.

Establishing the Scope and Defining the Vision of the Integrated System

In the early stages of integrated systems planning, whether at the local, state or federal levels, fundamental decisions need to be made regarding the nature, scope and objectives of the initiative. Although it is often common perception among decisionmakers that what is needed is an integrated *criminal justice system*, these boundaries are artificially narrow if the expectation is that it incorporates only law enforcement, prosecution, courts and corrections. Indeed, each of these constituent agencies has myriad other responsibilities, and their inter-relationships and need to exchange information with others represents the protean structure of the justice information enterprise.

In the earliest stages of integrated systems planning and implementation, it is crucial that a jurisdiction define a vision for the integrated system. That vision may be fairly broad in initial construction, provided it is translated into specific objectives that are attainable in the foreseeable future. The objectives will define what agencies and processes are to be included within the integration initiative, and they can be sufficiently narrow from a practical standpoint to enable successful completion and demonstrative benefits.

For example, the mission of the Pennsylvania Justice Network (JNET) is defined as:

> To enhance public safety through the integration of criminal justice information throughout the Commonwealth of Pennsylvania by adopting business practices which promote cost effectiveness, information sharing and timely and appropriate access to information while recognizing the independence of each agency.[7]

In Colorado, the mission of the integrated systems planning effort was stated as follows:

> Colorado Integrated Criminal Justice Information System (CICJIS) will establish an integrated computer information system which standardizes data and communications technology throughout the primary criminal justice community of interest: law enforcement, district attorneys, state funded courts, and state funded adult and youth corrections. It will facilitate tracking the complete life cycle of a criminal case through its various stages involving all criminal justice agencies. The case tracking will be accomplished without unnecessary duplication of data entry and data storage.[8]

Certainly, building the capacity to share information in an automated manner between the local police and/or sheriff’s department, prosecutor, court, correctional institution and probation agency is an important accomplishment. Nevertheless, it must ultimately extend beyond these institutions to such agencies as public defense, pretrial services, substance abuse treatment brokers, and potentially to city/county social services, education and other service

[7] *See* http://www.state.pa.us/Technology_Initiatives/jnet.home.htm

[8] *See* http://www.state.co.us/gov_dir/cicjis

agencies, if we are actually to realize the benefits of integrated information systems.

The mission defined for the Kansas Criminal Justice Information System Project is arguably broader:

> 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 noncriminal justice users that supports 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.[9]

Although these mission statements are fairly broad, the objectives articulated by the jurisdictions are more narrowly focused.

In Colorado, for example, "CICJIS, once implemented, will improve:

- Public safety by making more timely, accurate, and complete information concerning offenders available statewide to all criminal justice agencies and to individual decisionmakers in the system, including police officers, judges, and corrections officers;
- Decisionmaking by increasing the availability of statistical measures for evaluating public policy;
- Productivity of existing staff by reducing redundant data collection and input efforts among the agencies and by reducing or eliminating paper-based processing; and,
- Access to timely, accurate, and complete information by both criminal justice agency staff and the public."[10]

In Kansas, the objectives are defined as:

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

The contemporary move to community-based policing has been extended in many venues to a broader call for community-based government, and this move portends an important shift in information processing — toward more open systems. Community-based courts, such as the Midtown Manhattan Community Court, have demonstrated the importance of developing a comprehensive and integrated information system that is capable of incorporating criminal justice information (for example, state criminal history record, complaint), substance involvement information (for example, nature and severity of involvement), and treatment information (for example, treatment program options, performance, etc.) into a system that supports judicial decisionmaking and treatment programming, while reporting disposition data to both local law enforcement and the state criminal history records repository.

[9] *See* http://www.kbi.state.ks.us

[10] *See* http://www.state.co.us/gov_dir/cicjis

Governance Structure

One of the first steps in successful integrated systems planning is the establishment of appropriate governance bodies to provide vision, strategy and policy approval, and to provide oversight for implementation actions, such as acquisitions, major projects and studies. Governing bodies must identify key stakeholders and integration issues, break down barriers pertaining to access, privacy and technology, and stop turf battles before they begin. Key stakeholders must be engaged in the early stages of integrated systems planning so that they help define the effort, invest in its development, and recognize their continuing responsibility for its success.

Additionally, integration leaders should identify a champion — an Executive Sponsor — for the initiative who has sufficient voice within the community, clarity of vision, and the necessary organizational currency to bring leaders together and to press for commitments, decisions and support when necessary. Judges, state legislators, governors, mayors, council members, city managers and agency directors can make great champions. Champions must be visionary and charismatic leaders, as, in many cases, they form an essential bridge to the legislature, budget officials, agency heads, etc. Champions deal primarily with priority and funding issues, but they are also responsible for removing barriers encountered by implementation teams.

Governing Committees

The governing body should develop a strategic plan for the initiative. Planning should involve an intergovernmental representation of local, state and regional representatives who recognize the strategic importance of planning at the state and local levels, and understand and are knowledgeable about federal and national systems and requirements that must be linked to state and local programs. Federally supported integration initiatives can play an important role in developing strategies and standards that will greatly facilitate integration of local, regional and state systems to national and federal systems, and can lay the foundation for development of additional regional systems.

The experiences of various states regarding the creation of steering committees may be instructive. Some committees have been established through state statutes (for example, Colorado, Delaware, Kansas, North Carolina and Oregon), while others were created through executive orders (for example, Indiana and Michigan), or have come together without the need for legislative mandates (for example, Ohio and Pennsylvania). There is no single or correct way to form a statewide steering committee, and no two states have precisely the same committees in place, though there are common themes in general structure and issues addressed.

All jurisdictions recognize the importance of creating a governing body representing each of the agencies that are central players in the scope of the integrated system as conceived. Agency directors are typically appointed, though their designees are often, as a practical matter, allowed to serve as their proxy. Oregon's statute, for example, creates a Criminal Justice Information System Advisory Board, with the following members (or their designees):

- The State Court Administrator,
- The Director of the Department of Corrections,
- The Superintendent of State Police,
- The Executive Director of the Oregon Criminal Justice Commission,
- The Director of Transportation,
- The Chairperson of the State Board of Parole and Post-Prison Supervision,
- The Executive Director of the Board on Public Safety Standards and Training,
- A chief of police designated by the Oregon Association of Chiefs of Police,
- A sheriff designated by the Oregon Sheriffs Association,
- A jail manager designated by the Oregon Jail Managers Association, and
- The Administrator of the Information Resource Management Division of the Oregon Department of Administrative Services.[11]

Similarly, legislation in Kansas creates a statewide steering committee (the Criminal Justice

[11] Oregon Statutes §181.725(1).

Coordinating Council), representing the Governor, Attorney General, Director of the Kansas Bureau of Investigation, Secretary of Corrections, Chief Justice of the Supreme Court, Secretary of Social and Rehabilitation Services, and the Commissioner of Juvenile Justice.[12]

In Colorado, the integrated system was designed to link the information systems of five state agencies through use of a central index;[13] consequently, the legislation created a task force that was "comprised of the executive directors of the department of public safety, department of corrections, department of human services, the Colorado district attorneys' council and the state court administrator or their respective designees."[14]

Interestingly, the representatives described in the legislation deemed themselves an Executive Policy Board and maintained overall business authority of the system. They appointed a task force with the following members, since these individuals had a better feel for the day-to-day operations of each agency and would be in a better position to supervise systems development: Information System (IS) Director, Judicial Department; IS Director, Colorado District Attorneys' Council; IS Director, Department of Corrections; ITS Manager, Department of Youth Corrections; Systems Manager, Colorado Bureau of Investigations; and the CICJIS Chief Information Officer.

Even jurisdictions that do not rely on legislative authorization have incorporated a similar governing structure. In Pennsylvania, the integrated systems effort is guided by the JNET Steering Committee, a governor-appointed committee comprised of representatives of the following Commonwealth agencies:

- Administrative Office of the Pennsylvania Courts,
- Board of Pardons,
- Department of Corrections,
- Department of Public Welfare,
- Juvenile Court Judges' Commission,
- Office of the Attorney General,
- Pennsylvania Board of Probation and Parole,
- Pennsylvania Commission on Crime and Delinquency,
- Pennsylvania Department of Transportation, and the
- Pennsylvania State Police.[15]

These 10 Commonwealth agencies "will become the first users and will provide the initial content [for the integrated system] from their existing information systems. Other state, county, and local organizations will be encouraged to join as the capacity of the JNET System grows."[16]

A similar governance structure is warranted in local integration efforts where the directors of each of the principal participating agencies serve on the policy-level governing board. The critical point is that the governing board must represent the constituent agencies, and must include representatives who have the authority to commit and engage agency resources and priorities.

Subcommittees

Regardless whether the policy-level governance committee is legislatively appointed or convened at the request of the governor or the agency directors themselves, this committee is designed to address broad policy issues, secure sufficient resources to support the effort, and provide guidance and support to the overall effort. Operational and technical issues should be addressed by subcommittees appointed for the specific purposes of addressing these issues. Although the specific subcommittee structure varies by jurisdiction, there are again many common trends across jurisdictions.

Kansas has implemented a series of subcommittees to address technical and policy issues associated with their comprehensive integrated systems initiative. In addition to their CJIS Advisory Board, they have created the following subcommittees:[17]

[12] Article 95 — Kansas Criminal Justice Coordinating Council §74-9501(b).

[13] Those five state agencies are: Department of Human Services (Division of Youth Corrections), Department of Public Safety, Department of Corrections, State Court Administrator's Office, and the Colorado District Attorneys' Council.

[14] C.R.S. §16-20.5-103(1).

[15] *See* http://www.state.pa.us/Technology_Initiatives/jnet/home.htm

[16] Ibid.

[17] *See* http://www.kbi.state.ks.us/governance/default.asp

- Standards/Technology Task Force,
- AFIS Subcommittee,
- ASTRA Board (law enforcement telecommunications),
- Juvenile Justice Subcommittee,
- Incident-Based Reporting Subcommittee,
- Law Enforcement System Task Force,
- Prosecution System Task Force, and the
- Supervision System Task Force.

These subcommittees and task forces are organized to address specific technical, operational and policy issues associated with the integrated systems planning and implementation efforts, and they include both state and local agency representatives.

Similarly, the Florida Criminal and Juvenile Justice Information System Council formed five workgroups to address comparable issues:

- **Policies and Standards Work Group**, which developed a set of guiding principles for the efficient and effective sharing of criminal and juvenile justice information among users and providers throughout the state. The guiding principles were codified into law by the 1996 legislature;[18]
- **Juvenile Data Sharing Work Group**, which is focused on the requirements for mandatory reporting of juvenile disposition data;
- **Telecommunications Work Group**, which is planning, developing and installing a statewide telecommunications network for Florida criminal and juvenile justice agencies, known as the Criminal Justice Network (CJNet);
- **Federal Funding Work Group**, to evaluate federal funding opportunities and make recommendations to the Council regarding the most advantageous ways to use those funds for the benefit of the criminal justice community; and the
- **Sentencing Forms and Process Work Group**, which reviews the sentencing process and associated data and forms, and recommends to the Council any appropriate changes for improving the accuracy of data and information sharing, and reducing redundancy in records.[19]

The Colorado CICJIS task force created the following subcommittees to address specific issues associated with their integrated systems planning initiative:

- **Technical Work Group** (Data Dictionary Team), which is comprised of technical analyst/ programming staff from each of the five participating agencies, Sybase and the technical analyst staff member from the CICJIS project. This group is responsible for designing and implementing the CICJIS data dictionary, programming all transfers and applications, and building the system's Central Index.
- **Tactical Business Group**, which is comprised of on-line users from each of the five state agencies, local law enforcement, other involved agencies, and the business analyst staff member from the CICJIS project. This group is responsible for determining the processes, screens and programs that are viable solutions for on-line users. This group also tests applications upon completion and educates the CICJIS project staff on current procedures within their respective agencies and departments.

In addition, other entities support CICJIS development:

- **DCSIP (Drug Control System Improvement Program) Board**, which oversees the federal grant money administered by the Department of Criminal Justice (DCJ).
- **Strategic Business Work Group**, which is staffed by DCJ and also includes members of the CICJIS Task Force. This group looks at long-term strategic issues regarding CICJIS.

[18] *See* Fla. Stat. Ann. §943.081.

[19] *See*, Criminal and Juvenile Justice Information Systems Council, "Report to the Florida Legislature" (January 1998). (Photocopy of original document on file at SEARCH offices.)

The subcommittees will vary by jurisdiction, depending on the technical solutions embraced, the policy environment within which they work, and unique needs of the jurisdiction. Clearly, however, key technical and operational subcommittees must be established to address important technical issues, operational practices and policies, and business re-engineering. The shift to integrated systems means that we are doing business differently, and these technical and operational committees/task forces/working groups — which are comprised of the operational users, managers and technicians — are needed to define the way we are going to do it differently.

Conclusion

In organizing for integrated systems planning and implementation, jurisdictions must develop comprehensive plans for change and technology. The plans must begin with an understanding and defensible description of what integration of justice information means (from a functional and organizational standpoint), and an articulate vision of the goals and objectives of integration. In defining the nature and scope of integration, key stakeholders, users, contributors and technical support personnel of systems must invest in the project and participate in both policy and technical committees.

Beyond the fundamental organization and structural issues addressed, however, it is important to realize that organizing for change encompasses only the critical first steps in integrated systems planning and implementation. Once organized, the initiative must continue and address other issues, such as change management, long-term funding, inter-organizational working relationships, and emerging privacy, confidentiality and security issues.

Creating a Community of Value Around Criminal Justice: Digital Strategies for Funding Integration Efforts

By Steve E. Kolodney and Paul W. Taylor
Washington State Department of Information Services[1]

Steve E. Kolodney serves Governor Gary Locke as director of Washington State's Department of Information Services. He is the state's Chief Information Officer and a member of the Governor's Cabinet. In both 1997 and 1998, Washington was named the nation's "Digital State," ranking first in the annual 50-state survey that examines the use of digital technology to deliver government services.

Mr. Kolodney manages the state's computing and telecommunications facilities and is also responsible for information technology policy and oversight of the state's information technology resources.

Mr. Kolodney has worked in the information technology field for more than 25 years. In 1974, he was named Executive Director of SEARCH, where he worked with the states and the federal government to establish programs in justice information.

California Governor George Deukmejian named Mr. Kolodney director of the Office of Information Technology in 1983. In that position, he built the state's information technology program from $350 million to more than $1 billion per year.

Mr. Kolodney holds an MBA from the University of California, Berkeley. He is a Distinguished Special Lecturer in the School of Public Safety and Professional Studies, University of New Haven, and has been a faculty member at the School of Health and Human Services, California State University, Sacramento.

A single-funding model for criminal justice integration may be as elusive as a single-business model for the Internet. The search for such holy grails may trap us into projecting an imperfect present onto the future. Such an approach leads to the apparently inevitable conclusion that the current financial burden of maintaining discrete systems will become a budget buster as we move toward integration, but that's the wrong starting point. Instead, author James Burke contends that success in developing new models is contingent on "thinking backwards from the future, rather than tracing a path from here to there and becoming caught in the prediction trap."[2]

The defining characteristic of the future is digitization. Moreover, the potential for cutting costs and improving reach is in the DNA of digital technologies. The challenge is to seize the transformation power of digital technologies to create a sustainable approach to justice integration.

Larry Downes and Chunka Mui have articulated a series of "digital strategies"[3] that provide a framework for systematically "thinking backwards from the future." It is useful to see the formidable challenges of funding criminal justice integration through the lens of these digital strategies. Not all the strategies apply equally to the task before us but, when taken together, they define the emerging environment within which we will compete for resources.

Create communities of value

The real power of justice integration is that its architecture allows for high bandwidth and secures information exchange within the criminal justice community. While the Nicholas Negroponte formulation that "digits commingle effortlessly"[4] remains true, they will remain trapped within stovepipe systems

[1] Steve E. Kolodney, MBA, is director and Paul W. Taylor, Ph.D., is deputy director of the Washington State Department of Information Services. Dennis B. Hausman, Project Coordinator for the Washington State Justice Information Network, and Tom F. Wilson, R&G Associates, also contributed to this paper.

[2] James Burke, *Connections*, Boston: Little Brown & Co., 1978.

[3] Larry Downes and Chunka Mui, *Unleashing the Killer App: Digital strategies for market dominance*, Boston: Harvard Business School Press, 1998.

[4] Nicholas Negroponte, *Being Digital*, New York: Knopf, 1995.

unless purposeful actions are taken to break down such barriers.

It is encouraging to see criminal justice move from a community of interest to a community of value by acting together to protect and promote its most valuable and under-exploited asset — information. The information needs of the community mirror a slogan from the early days of cross-platform multi-media development: "Author once, play anywhere." Today, in an environment informed by the Internet, that notion is the new conventional wisdom. Not so in the early days of justice integration, when law enforcement and other agencies were collecting and entering the same data over and over again. With the passage of the *Criminal Justice Information Act* in 1984, justice agencies in Washington State had legislative direction to use networked technology to break down the data stovepipes. At the same time, a spike in the number of convictions — the result of other legislative changes initiated in response to increasing public demands for safe communities — was driving up workloads.

State and local policy makers formed a unique alliance to address these issues by re-engineering the information systems that supported the justice system, or the justice enterprise. The life blood of the most visible parts of the justice enterprise — police, courts and prisons — is timely and accurate information. While each justice agency had traditionally been concerned only with its individual mission, there was a growing recognition that each link was dependent on the others in the chain.[5]

The old model, under which justice information systems evolved separately with little concern about duplication of efforts or thoughts of sharing information with other members of the justice enterprise, was antithetical to the emerging demands for efficiency and responsiveness. The new model was embodied in the Washington State Justice Information Network (JIN). The JIN is concerned with the just-in-time availability of criminal history information regarding a suspect's identity and justice status at the appropriate intersections among formerly discrete systems. The utility curve is such that the more the information is shared, the more valuable it becomes. From the booking station to the court, and at all points in between, information can flow to all partners in the justice enterprise.

Based upon years of working together toward the establishment of the JIN, justice partners are setting aside historic turf issues in favor of a shared vision of an integrated future. Through the work of two widely representative committees — one executive, the other technical — the community has entered into formal agreements in areas of common concern. In Washington State, we have found it particularly useful to have neutral parties — first the state Office of Financial Management, now the Department of Information Services — act as coordinator of this statewide, multi-agency effort.

It has also been very useful to have a staff coordinator work on behalf of the community as a whole. Our coordinator has been able to build relationships among the players because, in this case, he has street credibility and independence. The "street cred" stems from years of service in the criminal justice community. The independence comes from the fact he gained that expertise somewhere else. The coordinator was not beholden, or seen to be beholden, to any one interest in the community. The community was involved in his recruitment, and it has some skin in the game — his salary is co-funded by five of the major players.

The result is that, the criminal justice community — including the full range of state and local interests[6] — committed itself to design or develop any system related to the state's integration effort without the effective participation of state and local stakeholders.

Other states have been very effective in creating a community of value with impressive results. Indeed, the North Carolina Bureau of Investigation used a task force approach to develop a global view of criminal justice and began allocating grant funds across the community of players in criminal justice. North Caro-

[5] Justice Information Strategic Plan 93-95 Update.

[6] The parties include the Department of Licensing, Department of Corrections, the Office of the Administrator for the Courts, the Washington State Patrol, the Office of the Attorney General, the Washington Association of County Officials, the Washington Association of Prosecuting Attorneys, the Washington Association of Sheriffs and Police Chiefs, the Association of Washington Cities, the Washington Association of Counties, and the Washington State Association of County Clerks.

lina now has 100 percent electronic disposition reporting from the courts because it made sure the courts got a share of the funds commensurate with providing full court disposition reporting to the repository. Clearly, it only happened because the merits of an enterprise approach were compelling enough to do the hard work of reallocating formerly discrete funding streams to a project that delivered real value to the larger community.

This same commitment to a community of value is also in evidence in a growing recognition that it not just acceptable, but desirable, for the U.S. Department of Justice (DOJ) to condition its federal grant-funding streams to ensure planning and development consistent with criminal justice integration. It is in the interests of all of us to allow the states to pool their resources to embrace statewide justice integration efforts. Doing anything less will continue to perpetuate stovepipe systems. At this time, it is clear that the federal vision is for a complete justice enterprise system; however, the funding model is for discrete projects.

Conditioning funds is important, but it is not enough by itself. We must urge federal granting agencies to allow states to pool grant funds to leverage integration efforts. North Carolina has demonstrated what can happen when funding is fully leveraged — but the exception needs to become the rule.

There is reason to be encouraged. For the first time, there are strong signals from the U.S. DOJ that it intends to coordinate integration funding among its granting agencies. Previously, each granting agency (for example, Bureau of Justice Statistics or BJS, Bureau of Justice Assistance or BJA, National Institute of Justice or NIJ) would award funding for stand-alone projects. A state agency might get awards from three different granting agencies, but the agency was not able to use the money toward one project. This funding practice forced agencies to devise three discrete projects of limited scope. It now appears that DOJ will allow the coordination of the grants to permit combined funding for a project big enough to make significant progress toward integration. As an example, it would be ideal to have a grant project called "improving identification and criminal history availability." Within that project, funds could be allocated to law enforcement, prosecution, courts and corrections to fund integration of an Automated Fingerprint Identification System (AFIS)/live-scan network, full electronic arrest and disposition reporting, and correctional status information.

There is also reason to remain vigilant. The federal vision is for enterprise systems, but the funding model remains tied to discrete projects for now. Without meaningful change, the grant award models will perpetuate stovepipe systems and thwart innovation — and integration.

Structure every transaction as a joint venture

Justice integration assumes that every transaction is a joint venture among members of the community of value. Downes and Mui contend that, "Soon you will be able to treat basic transactions with the same attention you would a complex joint venture, bringing the best set of business partners and allocating work, risk and ownership as best suited."[7]

Outsource to the customer and treat each customer as a market segment of one

The criminal justice community has not historically seen itself in terms of customers or market segments. At one level, "customer" may mean the officer in the patrol car or the local jailer or clerk. Clearly, they are important; the asset of information is created at the local level. As discussed below, the value of integrated criminal justice is a function of its ability to provide affordable points of entry for local data. Each officer, jailer and clerk is indeed a market segment of one, each making custom requests, many in an uncontrolled environment.

We also need to think about customers outside the community. These are customers in the traditional sense — citizens, consumers and people. In his new book "Telecosm," George Gilder reminds us that "the microchip shifted power within organizations and facilitated new organizations." In fact, criminal justice integration is one of those new organizations. But Gilder also contends that "the telecosm goes further and shifts power from organizations to [individuals]."[8]

Gilder's vision of a telecosm

[7] Ibid., at 133.

[8] Interview with George Gilder, *The Hollywood Reporter, New Media V: Information Technology Special Issue*, November 1998.

represents both challenges and opportunities for the criminal justice community. How will we respond to the growing expectation of direct citizen access to information about an individual's safety rather than the public's safety? Blame it on the World Wide Web, but expectations have changed. It is not much of a reach to suggest that an individual looking for a new home for her family expects to be able to find a home, shop for a mortgage, and check crime statistics for a given neighborhood.

The criminal justice community can be the first to seize these opportunities and their related revenue streams, or it can forfeit the opportunities to private-sector information resellers. The term of art for all of this is "reintermediation" — our challenge is to make purposeful decisions about whether to engage this new arena of "mass customization" before the opportunity is lost to more aggressive players.

Cannibalize your markets

If we were constantly in the position of defending rising operating costs to the budget office, city council or legislature, Downes and Mui would suggest that it is time to deliberately cannibalize our markets.

The message here is to stop defending the indefensible. It will free time and resources to defend what is truly important and allow us to reallocate those resources toward building our collective future, even if it means letting go of parts of our past.

Digital technologies can reduce transaction costs from dollars to pennies if we are prepared to change our cost model. Change brings with it difficult decisions, but the potential payoff is enormous. It affords us the opportunity to leverage our shared infrastructure and provides an inexpensive point of entry for the full range of criminal justice partners.

We will be unable to bring the cost of entry down if we accept the inefficiencies of stovepipe processes and systems. We cannot afford to have local governments, law enforcement agencies and state agencies compete among themselves, and with each other, for limited federal funding. Instead of working together toward common goals, those vying for funds become combatants and withdraw from the mission of integrated justice.

Destroy your value chain

Here again, the term is largely foreign to the criminal justice community. Destroying one's value chain has also been called "creative destruction," a Phoenix-rising-from-the-ashes concept that hastens the end of old ways.

Some of the old ways are significant barriers to moving forward, including:

- Uncoordinated investments in technology resulting in a hodge-podge of separate systems with limited use;
- Islands of information existing without connectivity, limiting the use of the data being collected; and,
- The continuing need to extract data and to put it into a format that is useful by other agencies.

The old ways are often products of historical circumstances and historical accidents. Many of those circumstances have changed, and digital technology holds the potential to transform the underlying business processes. The goal here is not continuous improvement, but continuous innovation.

Ensure continuity for the customer, not yourself, and replace rude interfaces with learning interfaces

The transformation of low-value, high-volume processes is a key component of changing the cost structure, thereby making integration the affordable alternative. An industry report on police justice and information correctly concluded that:

> In an era in which the importance of community-oriented policing is acknowledged, public safety agencies can no longer tolerate such inefficient processes which result in their officers spending their time filling in paperwork instead of working in the community which they serve.[9]

Recognizing that members of the criminal justice community have already made significant investments in information technology systems, how do we deliver on the efficiency promises of integration?

In Washington State, the answer appears deceptively simple: a process control number (PCN). The community of interest came together and defined those data elements that needed to be shared among partnering agencies to eliminate

[9] Andrew Ward, *Police Justice and Identification*, IBM Reports 1998-1999.

the extraordinary duplicative effort of data entry from one jurisdiction to another.

The development of the PCN would have been impossible if not for a shared commitment to the goals of criminal justice. Not everyone got everything they wanted, but the community as a whole got what it needed. The PCN informs the development of the infrastructure — from digital live-scan finger image machines at booking stations to case management systems in the courts. Importantly, the PCN leverages existing investments in formerly discrete systems by integration partners.

As importantly, the integration effort can only deliver on its promise with uniform adherence to the PCN as well as common network protocols (Transmission Control Protocol/Internet Protocol or TCP/IP). These protocols break down the old data stovepipes and create an environment within which digits can commingle effortlessly.

Give away as much information as you can

Successful integration lends itself to the promise that digital information increases in value as it is shared widely and effectively within the community and beyond. To their credit, many of the existing federal funding programs are entirely consistent with the digital strategy of giving away as much information as you can. For example:

- The BJA Edward Byrne Memorial State and Local Law Enforcement Assistance Program funds projects that are multi-jurisdictional in scope. The Byrne Discretionary Grant Program targets projects related to crime, and violence prevention and control.
- Byrne Formula Grants are awarded to states and territories, which in turn make subgrant awards to local units of government. These subgrants may be used to fund information systems that support the widespread apprehension, prosecution and rehabilitation of criminals.
- The BJS's National Criminal History Improvement Program (NCHIP) is an umbrella program designed to assist states in meeting evolving federal and state requirements involving criminal history and related records, such as protective orders and sexual offender registry records. Funds may be used for technical assistance to support interfaces between states and national records systems.
- The Local Law Enforcement Block Grant Program provides local jurisdictions with up to $10,000 to acquire information technology.
- BJA also administers a number of grants for community courts and local law enforcement equipment.

Justice integration and the widespread "giving away" of information are at the heart of the newest federal funding initiative. Pending appropriations, U.S. DOJ will provide grants under the *Crime Identification Technology Act of 1998* to establish or upgrade an integrated approach to develop information and identification technologies. Under the program, $250 million a year for 5 years beginning in Fiscal Year 1999 is expected to be available to upgrade existing criminal history and justice systems, and to promote compatibility among national, state and local systems.

Treat your assets as liabilities

Just as the Internet has trumped proprietary networks and electronic commerce is shaking the retail sector at its foundation, the criminal justice community must reassess the value of what it has traditionally seen as assets. That means changing our cost models and investing in the infrastructure of the future, even if it means sacrificing part of the past. Witness, for example, the privatization of correctional facilities in some jurisdictions — a recognition that there were areas where owning the asset was not in the best interest of the taxpayer.

Similarly, cost-benefit analysis for stand-alone information technology systems in criminal justice crumble under the weight of the total cost of ownership. When those costs are shared through integration, partners get all the value that a stovepipe system would provide but the risks and rewards of refurbishment, maintenance and upgrades are amortized across the consortium.

Manage innovation as a portfolio of options

Downes and Mui encourage an investment view of possible alternatives, recommending that we should "manage innovation as a portfolio of options. [Information technology (IT) budgets] could be managed, not as a series of discrete projects, but as a *portfolio*." We have done significant work in developing a portfolio view of IT investments across state government in Washington.

The portfolio view brings you back to what assets you have in common, and those common assets are the truly important ones. In a word, it's the network, a network that is sufficiently robust and nimble to respond to the changing needs of the criminal justice community.

We are encouraged by the recent BJA grant to the organization that represents state Chief Information Officers (CIO) to examine the network architecture needed to support justice integration. The National Association of State Information Resource Executives (NASIRE) will examine state criminal justice architectures and develop best practices for interoperability and data sharing among local governments. As reported, "The study initially will focus on information exchange and system integration among law enforcement, but it has even broader information-sharing implications for a host of criminal justice agencies, such as the courts and state attorney offices."

As CIOs, we are interested in how the criminal justice exchanges relate to the larger movement of information within the state.

The impact of digital strategies on funding integration

The promise of criminal justice integration remains compelling and has become ever more important in an increasingly complex, connected and — in some cases — hostile world.

The technology exists today to deliver on the promise in ways that were the stuff of science fiction just a few short years ago. *Government Technology* magazine explored the state of the art in criminal justice integration in a three-part series of cover stories that ran from December 1998 through February 1999.

The series has focused as much on the relationships necessary to make integration work as it did on technology. But technology is forcing changes to relationships, and that is the final point made by Downes and Mui. Technology is "disruptive"; it must, and it will, disrupt funding models. As discussed earlier, federal funding agencies have made a commitment to redirecting formerly discrete funding streams into an integration pool.

North Carolina has managed to break down the funding stovepipes too. Former New York Governor Mario Cuomo was also thinking digitally years ago when he created the Governor's Integration Improvement Fund. The then-governor had an integration fee applied to fines and registrations. The governor also chaired a task force of principal players from the criminal justice community. Money was allocated in fair shares to those agencies that worked toward integration. The approach demonstrated a deep commitment of the governor to criminal justice and provided an ongoing source of funds for integration. The flexibility of such an improvement fund provides a much-needed bridge between stovepipe funding streams.

Consider the Byrne Fund paradox. Washington State received approximately $10 million in Byrne funds in Fiscal Year 1998. The formula grants are earmarked for improvements to criminal justice systems in support of enforcement against drug trafficking, violent crimes and serious offenses. Of the funds, only 5 percent are set aside for criminal history record improvement programs.

As a practical matter, JIN planners have a direct role in deciding how the set-aside is used. The network governing bodies work with the Office of Financial Management to determine how best to allocate the set-aside toward the network's priorities each year. Contrast that with the allocation of 95 percent of the Byrne funds. Those funds flow through the state Department of Community, Trade and Economic Development (CTED). The department works with many of the same criminal justice agencies involved with JIN — but not JIN itself — in allocating the lion's share of the Byrne funds. The process involves setting spending priorities in 26 areas (11 of which are actually targeted by the CTED Board of Directors) with a lead-time of up to two and a half years.

The mandated process is counterproductive to integration efforts, and will not stand under the onslaught of digital technologies and the attendant public expectations.

Until the central funding mechanisms change, we will have to look to the periphery for innovation. Funding streams are not likely to grow markedly in the foreseeable future, but it is unclear that a shortage of money is the problem. It may well be that funds are sufficient but out of reach because of an out-of-date process. It is incumbent on the criminal justice community to use the available funding more effectively. In the words of Downes and Mui, “Enhancing communities … will create the best opportunities to extract new margins.”[10] Those new margins will fuel our efforts to move toward criminal justice integration.

In addition to the New York and North Carolina examples, the Washington State experience with network integration in other sectors illustrates the potential to meet the objectives of criminal justice integration through a revolving fund. Federal grants would continue to be applied toward a coordinated set of acquisition activities among partners. State appropriations, as available, would offset the transport costs of sharing the data on the network. Each partner would be required to make co-pays to an internal service fund to support the ongoing maintenance and refurbishment of network resources. Under such a plan, partners would have access to the justice network without discrimination based on geographical distance. The co-pays would also provide low-cost points of entry for even the smallest jail or detachment. The greater the number of local entities providing data, the greater the value of the shared information and the network itself.

The community of value around criminal justice must find a sustainable funding mechanism. There is really no lack of funds, but much of the money is locked in stovepipes. In the short term, stovepipes threaten integration. In the long term, burdensome administrative processes will collapse under their own weight; they will not withstand the demands of the digital economy. If we seize this moment and topple a few stovepipes ourselves, we can take our place on the right side of history.

[10] Ibid., at 109.

Technology Issues and Challenges

By Robert L. Marx
Senior System Specialist
SEARCH, The National Consortium for Justice Information and Statistics

Robert L. Marx has been associated with SEARCH since its inception in 1969. He currently serves as Senior System Specialist, with particular emphasis on automated fingerprint identification systems (AFIS) and the design, analysis and evaluation of information systems in state identification bureaus.

Mr. Marx has provided consulting services to numerous state and local governments, as well as to the U.S. Senate; the Congressional Office of Technology Assessment; the Office of Telecommunications Policy; the Law Enforcement Assistance Administration; and the Bureau of Justice Statistics, U.S. Department of Justice.

Mr. Marx has addressed previous SEARCH national conferences on a variety of technical matters, and has written extensively on technical issues associated with the design and implementation of AFIS.

Mr. Marx earned a B.S. in Chemistry from Marquette University and completed graduate work in Physics at the United States Naval Postgraduate School.

1. The Operational Context of Technology

Technology, as interesting and fun as it is, does not exist in an intellectual vacuum. Technology is appropriate or inappropriate insofar as it contributes to or detracts from the achievement of an operational objective.

It is *not* an operational objective to construct a high-speed intranet. It is an operational objective to provide prosecutors with the information they need in order to conduct a case, regardless of where that information was collected or stored.

It is *not* an operational objective to provide an archive of mugshots in JPEG[1] format. It is an operational objective to make mugshots available to crime investigators during witness interrogations.

Therefore, the first step in system implementation is not to select technology, but to articulate *objectives*. If we don't decide at the outset what we are attempting to do, how will we ever know if we have finished?

Those of us who inhabit the real world know that we do not really operate in this fashion at all times. Often, we simply assume that the operational requirements previously identified and embedded in our existing systems remain valid, and we jump immediately to the second (and easier) step in technology usage, namely:

- More, more, more,
- Faster, faster, faster,
- Cheaper, cheaper, cheaper.

If we have a collection of 100,000 mugshots, we aim for a half-million; if we have been providing telecommunication services at 9600 bits per second, we aim for 56 kilobits per second; if we have been passing on to our users a monthly connection charge of $1,000, we aim for $400. Since words like "more," "faster" and "cheaper" are subject to widespread understanding by outsiders, we have substituted the terms "scalability," "performance index" and "price-performance index" to keep the discussion contained within the fraternity of systems professionals.

Do you know what? Much of the time the more-faster-cheaper decision is a valid one. Operational needs remain relatively stable over years and even decades, and if the needs were being met in the past, it may be necessary only to support those same requirements by providing the same information products, only more of it delivered faster for less money.

One of the more attractive features of such an approach to

[1] Joint Photographic Expert Group.

system upgrades is that, in most cases, it is not career-risking behavior for the technical people who support it. Given the amazing implications of Moore's Law (named after Gordon Moore of Intel and proved valid over two decades) and its various corollaries, systems people have come to rightly expect that processor power will double every 18 months, that disk capacity will double every 2 years, that network speeds will double every 3 or 4 years, that hardware prices will drop 20 percent per year, and so forth. If one adopts the more-faster-cheaper goals of system improvement, the probability of successful upgrade — to use the jargon of me and my consultant colleagues — "asymptotically approaches unity" or, more simply put, is "danged near a sure thing."

This more-faster-cheaper technique sometimes leads to unfortunate results, including the propagation into the future of design decisions made decades ago and no longer valid simply because changing previous decisions does not comply with the more-faster-cheaper mantra. For example, some time during 1999 a very major system rewrite will be completed in which all printed and displayed output of the system will be expressed entirely in uppercase characters. Is this because new social science research determined that people find it easier to read uppercase text than mixed-case text? No. Is it because the 1,200-year experiment with lowercase letters is nearing completion and may be suspended pending a full evaluation? No. It is because change is dangerous. Perhaps some user, or even many users, will have to scrap their 1957-era Model 28 teletypes and will scream. Perhaps the present long-term users of the system, having never seen lowercase letters, would require retraining. Perhaps there is no safe way to convert the legacy database to mixed-case, and perhaps reports which are partially all-caps and partially mixed-case are deemed by a review panel to be aesthetically repugnant to users. More-faster-cheaper may seem to be an optimal strategy for the risk-averse; but it almost never results in improvements to the underlying operational efforts of criminal justice practitioners.

However, this symposium is for a different sort of person. I look into your faces and see the descendants of those intrepid mariners who lashed themselves to the masts of the clipper ships and sailed into Pacific storms to gain the precious minutes and hours which would result in victory in the annual race to bring the first casks of tea from Shanghai to San Francisco. Yes, many of those brave souls lost their ships, their careers and even their lives in the attempt. But what is financial ruin, loss of livelihood and death compared to honor, do you not agree?

But wait just a moment. I notice a few in the audience who do not appear as enthusiastic about the lashed-to-the-mast scenario as I had originally believed. So let us consider a second general approach to system improvement, which I shall call the "technology-driven musing," or TDM approach. This method starts with some new technology becoming available. The geo-positioning satellite (GPS) system provides a nice example. This technology, originally developed for military purposes with little regard for price and maximum regard for performance, has for some years been available in the civilian market at ever-decreasing prices. Where should this technology fit into the criminal justice toolkit? Maybe it should be built into mobile radio equipment so that every police message is "tagged" with the location of the police vehicle. Maybe it should be used in vehicle tailing kits, or incorporated into cell phones to permit automated redirection of 911 calls to the appropriate law enforcement agency. It is in this way that TDM sometimes leads to new operational requirements that can only be met by the new technology that was the subject of the musing.

Anyone who reads the computer trade press regularly knows there is no lack of new technology to fuel the musing — smart cards and iris scanners, digital signatures, eXtensible Markup Language (XML), public key encryption, palm computers, clocks that calibrate themselves by listening to the national-standard atomic clocks, data warehouses and datamarts, facial recognition, and so on.

The TDM approach leads to new operational requirements or, at a minimum, to radically new ways of meeting old operational requirements. There are real risks in this approach. The technology may be at too early a stage of development, or the market may be too ephemeral to drive the price down, or there may be flaws in the technology that will be noticed only too late, or the requirement may be more in the eye of the provider than in the eye of the potential customers. The upside potential can be very high, but the downside potential can also be substantial. Whereas the more-faster-cheaper approach to development is for those who crave the melatonin resulting from a long walk on a quiet country road, TDM is for those who crave the pain-numbing endorphins resulting from a marathon run.

As my eyes adjust to the illumination levels of this room, I notice a third type of person present; in fact, I notice that the majority of us here are of this third type. We read the trade press and pay attention to new product announcements. We pay attention to prices. We spend a lot of time watching criminal justice practitioners, seeing how they do things, wondering if there are better ways to do those things, wondering if there are other things they could be doing. We listen a lot and we talk a little. We document procedures and think about changing procedures to reduce the training required to do them, to reduce their labor content, to smooth the interface between one process and another. We trust our experience. We keep track of what our colleagues in other cities and counties and states are doing, what works and what does not. We avoid unnecessary risk but we take risks if justified by the potential for system improvement. We don't really have a name for what we do, but since the risk-averse and the risk-attracted guys have snappy names, we will call our technique the "simply professional approach," or SPA. People who look for more-faster-cheaper in our work find it; those who look for technology-driven musing find that; but we know that we are just pragmatic professionals.

As pragmatic professionals, we understand the relationship between technology and operational objectives. First, technology allows us to achieve present operational objectives on a larger scale, faster and less expensively. Second, technology allows us to conceive, describe, propose and adopt new objectives not previously attainable.

2. Describing and Changing Business Processes

Notice that, up to this point, we have discussed how we approach our system development tasks, what motivates us to begin and what general assumptions we bring to our task. We have not considered how we do things; that is, we have not described our *business processes*. We need a clear understanding of how we do things now, with our present system (or non-system).

Business process documentation requires:

(a) enumeration of the operational processes we have (for example, arraignment, charging, witness notification),

(b) how often we do each process (for example, per month or year),

(c) what participants are involved (for example, defense attorney, defendant and judge), and

(d) what is done (for example, the steps undertaken, the data collected and used).

But business process documentation is not a direct input to the design process; it is merely an "investigative lead" in preparation for the task of *business process re-engineering*. BPR, as it is called, considers the objectives of each business process, available technology, and other factors, and proposes a new way of accomplishing the same objectives. For example, the arraignment business process might be re-engineered to use video equipment instead of a bus to bring all the participants into a single "place" for the arraignment.

Now wait just a darned minute. Why should the operational folks change the way they do things just to fit in with some computer junkie's idea of how they should do things? Well, they shouldn't. But neither should they continue to do things the way they have always done them simply because that is the way they've always done them. This is a golden time to examine processes with eyes open wide. For each process, ask yourself the following:

- What are we trying to accomplish here?
- Why do we do it this way? What other ways are there to do this?
- Are our methods a reflection of past and present technical limitations in our system that could be removed?
- Would other methods reduce the labor content of the process, or reduce the training requirement for it, or make the process results available more quickly, or provide new benefits not attainable with the existing process?

One documentation technique is Workflow Analysis. The business process is decomposed into tasks. Each task has a list of participants, materials and information needed, task methods and a task output. Tasks are fitted together into a workflow model that shows the situation under which a task is performed, how often it is performed, and the destination of the task product.

The BPR process requires a peek at technology. Technology, at least sometimes, provides empowerment to BPR. Video conference technology can empower a county to re-engineer the arraignment business process, or empower a state to institute remote testimony by fingerprint examiners. Automated fingerprint identification technology can empower a police department to identify crime perpetrators and to streamline the arrest booking process. Extranet technology can empower a court to re-engineer the way private attorneys, victims and witnesses are kept abreast of court case status.

Profound understanding of every technology is not required at this point in the process. A general sense of what is available and what is becoming available is sufficient. Where is one to get this general sense? Vendors can provide it. Criminal justice consultants can provide it. Specialized magazines can provide it. Contact with peers in other counties and states can provide it. This symposium session can provide it.

What should we look for in the BPR process?

I would treat every multi-part form as a suspect, especially if the data on the form is typed rather than hand-written. If it is typed, is the data from the white (top) copy going to be key-entered into a system? How about the identical data from the blue copy and the canary copy and the peach copy? Maybe we should do something about that.

I would treat every paper document, whether multi-part or not, as a suspect. Is there a paperless way to transmit and store the information? How long is the information current and how long must it be kept?

I would treat every signature on a document as suspect. Of course, there are times when a document, even an electronic document, is going outside the normal paths of information flow, and a physical signature may be needed to prove its authenticity. More often, I believe, the signature is present as a simple way of telling who prepared the document rather than a voucher for its authenticity, and there are alternatives to a signature (a badge number, for example).

I would treat every meeting as suspect. Some meetings are conversational and deliberative in form and physical propinquity is helpful or even necessary. Often, however, a meeting is held to transfer custody of a document, or to announce a decision taken earlier, or to arrange a mutually agreeable time for yet another meeting; in those cases, the meetings can be virtual rather than physical.

I would observe and record the use of photocopy machines within the current process. Why are additional copies of documents needed, how long do they remain useful, and where do they go to die?

BPR is difficult to do, and done too seldomly, because it threatens the social fabric of the criminal justice community. The relationships among judges, clerks, bailiffs, attorneys, paralegals, police officers, jailers and others are as stable and important to the sense of well-being of their community as the relationships that bound together the medieval fiefs or that bind together military forces. But when it is done wisely and with sensitivity, BPR can improve the lives of all members of the community, including both the practitioners and the defendants.

If we skip the BPR step, we are reduced to following the more-faster-cheaper path I outlined earlier. That is, we fall back on the business process analysis results describing the current processes (you did do that at least, didn't you?). If we have completed BPR, we use those results. In either case, it is the business processes that anchor the system objectives we are about to discuss, and the system objectives in turn which describe the kickable, paintable reality we are setting out to build: our new system.

3. Stating Objectives

At some point, regardless of the methods and motivations that we use to get there, we must state our objectives; that is, we have to know what we are setting out to build, in part so we will know when to stop building.

Manufacturers have developed the concept of the "parts explosion." This is a hierarchical outline of product components. For example, the highest-level entry in a parts explosion diagram may be a *1999 Toyota Camry Sedan*. The second level might show *drive train*, *engine*, *frame* and *skin*, and perhaps a few more entities. The third level might show *transaxle*, *A-joint*, and so on. Eventually, perhaps at the eighth level, we get to bolts, nuts and screws and other components that do not themselves have further components. These parts-explosion diagrams have been found to be invaluable in defining a product and planning for its manufacture. We have borrowed this concept and converted it into an *objectives explosion diagram* which assures by its very structure that we have considered all the needs for a system, and have organized them systematically.

It is traditional and useful to state each objective succinctly, usually in a single declarative sentence without subordinate clauses. Thus, "Provide case management support to the county prosecutor" is better than "Effectuate an information-rich environment in which assistant district attorneys can operate effectively and efficiently in pursuit of justice for all the residents of our county."

It is traditional to call the top-level objective the *system goal*. The system goal is defined as the sum of all the objectives listed in the layers below it, and achievement of the system goal is dependent on achievement of each and every lower-level objective.

If we get the objectives right, we can get the high-level design right; if we get the high-level design right, we can get the detail design right. If we get the objectives right, we can get the acceptance test design right; if we get the acceptance test design right, we know that we have built or procured the system we set out to build or procure. What is left thereafter is merely to turn the system over to its users, watching always to see how they use and misuse it, what is missing, what is suboptimal, and what is just fine.

Suppose the system goal is to "Provide case management information for criminal justice cases in this county." Some see in an objectives explosion a tree-like structure in which the system goal is the trunk. (One could note that converting the objectives explosion diagram into a tree diagram requires that the tree root be at the top of the page while the tree twigs and leaves are at the bottom of the page. Then again, if one is going to get hung up on inconsequential details like this, perhaps one does not belong in the systems business.) High-level objectives are attached directly to the trunk. Examples are "Provide case management information to circuit court personnel" or "Provide case management information to police department personnel." Lower-order objectives attach to these branches (for example, "Provide national-level criminal history information upon request"), and in turn have even lower-order objectives attached to them, until we arrive at the outermost, lowest-order objectives, often called twigs or leaves. It is these branches, twigs and leaves, taken collectively, which describe the *functional requirements* of the system.

Note that the statement of objectives, or the statement of functional requirements, or the objective tree, or whatever we want to call the interim product at this point, is not expressed in technological terms. Technology may have influenced our original thinking about certain objectives; technology may have given us confidence that we could achieve certain objectives; technology may have been in the back of our minds as we searched for precise language in which to state certain objectives. But the objectives are not technological in nature, and we will not measure our eventual success or failure by a technological yardstick.

4. Technology, Standards and the Development Process

Eventually, we come to the point when we have finished our musing, finished our analysis and re-engineering of business processes, and finished our statement of objectives. It's time to build something. It's time to think about square feet and kilowatts and BTUs and stuff you can kick and paint. It's time to really think about technology, and it's time to think about standards.

Standards are what makes us confident that Tab A will fit into Slot B, that the nut will fit the bolt, that the plug on the workstation will fit into the receptacle on the wall. We live our ordinary lives surrounded by standards, which, to a great extent, is what makes our ordinary lives ordinary. If every receptacle provided a different voltage, every ream of paper was of a different size, every car required a different fuel, every fax machine a different coding structure — then every day would be an extraordinary day. Our lives would be not enriched but impoverished by the resulting diversity.

If one were setting out to purchase bolts and nuts, one would not normally require that the nuts be manufactured by the same firm as the bolts. Instead, one relies on a standard to describe the characteristics of the nuts and bolts, the diameter, thread pitch and depth, head shape and so forth. If the nut and bolt are made to the same standard, they will fit together properly.

So it is with standards in the information technology area. If two systems use the standard ASCII[2] character set, then both will interpret the bit-pattern 0010 0000 as the “space” character. If two systems use standard Java language, the byte-code for a program can be run on a wide variety of computer hardware. If two peripheral devices, say a printer and a scanner, both use the Universal Serial Bus (USB) connector, they can be connected to any USB-enabled computer and to each other.

All standards are not created equal.

Some standards, called *proprietary standards*, are not standards at all, in my opinion. Word processor file formats are a case in point. The file formats, in general, are not published, and when the manufacturer provides the technical details to a developer, it is usually under the terms of a confidentiality agreement. Proprietary standards tend to be unstable over time; Release 5.1 of the software will incorporate a completely different file structure that cannot be read by previous releases of the same product. There may be times when it is necessary to incorporate proprietary standards into one’s system, but when it is possible to avoid this practice, even at a substantial price in the original procurement, it should be avoided.

Sometimes one comes across the term *de facto standards*. As far as I can tell, these are proprietary standards that have a substantial market share. De facto standards do not provide any benefits over other proprietary standards, and should be treated with at least a modicum of disdain.

Other standards, called *industry standards*, have published characteristics but are not under the oversight of a standards body. The parallel printer plug, originally called the Centronics plug, remained stable for two decades. Because there is no adoption method for an industry standard other than the gradual widespread use by many vendors, there is no mechanism in place for gradual and sustained change to the standard, and so industry standards are more prone to disappear than they are to be modified.

Still other standards, the ones of most interest to present-day system designers, are *open standards*. They are usually developed by persons drawn from a broad background, often representing multiple vendors and academics. There is usually a previously established method, controlled by an independent standards group, by which the user community is kept informed during the standard-creating period, and by which interested parties can make their thoughts known to the persons actually doing the work. Interim drafts are submitted to broad review and criticism. There is almost always a formal adoption procedure that insures consensus among the affected and interested parties. Sometimes the standard provides formal test procedures to assure conformance to the standard, and occasionally there is a certification process established. Finally, there is a formal method of review and revision set up within the standard-setting process itself.

Multiple vendors often participate in the standard-setting process and later bring products to market in conformance with the standard. They compete on price, availability of product, additional features not called out in the standard, availability, quality and other product characteristics.

Open standards provide many important benefits to customers. Multiple sources hinder the planned-obsolescence marketing model embraced by some monopolistic vendors. Subsystems from different vendors can be made to operate as a single system. Systems can be linked together to form supersystems.

5. Some Standards-based Design Decisions

At this point in the process, we know the business processes we are trying to support, we know in a very formal way the goal and objectives of the systems we are going to build, and we have made a decision to construct our system using open standards wherever feasible. Now it’s time to start making serious decisions about the building blocks we will use for our system. We start with the least controversial decisions to be made, those in which the technical direction is well focused and supported by a broad consensus of our systems peers.

Some technological trends are so well established that a system designer begins the design process with a default decision to incorporate them. Of course, default decisions can be overridden as the design process continues.

Use of a relational database structure is one such default decision. The default might be altered to support an object-

[2] American Standard Code for Information Interchange.

oriented database structure, but almost certainly not to support a flat file structure, which is considered obsolete. Standard Query Language (SQL) is an open standard in this area. We may decide to insist that only standard SQL operators be used in our system, or we have accepted some proprietary extensions.

Use of object-oriented programming languages is becoming more prevalent and is approaching the default decision category. C++ and Java are open standards in this area.

Use of intranet technology for the telecommunication services of the system is another default judgement. Transmission Control Protocol (TCP) and Internet Protocol (IP) are open standards in this area. IP, in particular, is becoming nearly the universal choice, not only for data transfers but also for video and voice applications.

Use of World Wide Web technology is rapidly becoming such a default decision. HyperText Transfer Protocol (HTTP), HyperText Markup Language (HTML), and XML are open standards in this area. It is probably unnecessary to specify a single brand-name Web browser if one insists on staying within the confines of the HTTP-HTML-XML standards without proprietary extensions.

Use of magnetic disk file-stores of photographic data are increasingly common for mugshots, tattoo photographs, etc. Random Array of Independent Disks (RAID) and JPEG are open standards in this area.

There is an open international standard for the design of systems, often called the seven-layer system model. The standard is a bit long in the tooth, and suffers from a certain lack of clarity in some areas. However, it has had its effect on system design, especially in the sense that good designs today always try to separate the various levels of functionality rather than merge everything into the spaghetti-code of earlier times. Two-level and three-level client server software exhibits this separation, where presentation runs on the client machine, business rules may reside on another machine, calculations on another and database services on yet another machine.

Newer designs do not assume that the client has any special-purpose software, relying on generic Web browser software to provide the look-and-feel of the system. The newest designs do not assume a human user at all; my system and your system, can, without human intervention, find out about each others' existence, discover what sharable information each has, check for suitable permissions to share data, and then share data. Those of you who connect court case management systems to the state criminal history system for the reporting of dispositions employ an early version of this concept, but the technology is still in its infancy. Wise developers will assure that lights-out inter-computer data sharing is provided for in new system designs.

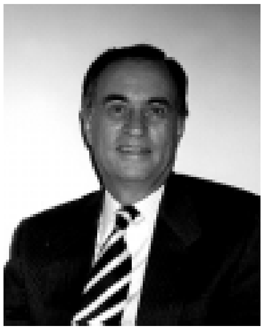
6. Conclusions

Technology is the servant of operational objectives, but technology also allows the identification of new operational objectives, and new ways of achieving objectives already identified.

Nearly all new technologies are non-standardized at their first appearance, but many become standardized very early.

Standards have been castigated at times as the enemies of innovation. I do not agree. There is ample room for innovation arising from the inventive interconnection of standardized parts.

Standards are surely important even in system environments under the control of a single agency. For interagency integration, standards are necessary.



Managing the Integrated System for the Long Term

By Paul Leuba
Senior Consultant, IBM Corporation

In an information technology career that has spanned more than 30 years, Paul Leuba has held a variety of technical and management positions responsible for developing and operating leading-edge computerized information systems in the criminal justice field.

Since joining IBM in January 1997, Mr. Leuba has served in a senior consulting role on several major criminal justice system integration projects, including the development of an integrated justice systems architecture for the Republic of South Africa. Prior to joining IBM, he directed Data Services for the Maryland Department of Public Safety and Correctional Services, where he oversaw the development and operation of Maryland's criminal justice information system over a 17-year period.

Mr. Leuba, a lifelong Maryland resident, graduated from Johns Hopkins University in Baltimore with a Bachelor of Science in Industrial Engineering. He is a member of the National Engineering Honor Society, TAU BETA PI.

I. Maintaining Criminal Justice Information Systems

The Essential Objectives

A maintenance strategy for criminal justice information systems must achieve two objectives in order to provide for long-term success. First and foremost, a maintenance and support services program must ensure that the system deliver value every day by efficiently supporting the organization's operational mandate. Increasingly, public safety and justice agencies rely on computerized information systems for mission-critical services. To achieve success, a maintenance program designed for a criminal justice agency's information systems must ensure that the system remains *relevant, reliable* and *responsive*. The system must deliver the right information to the right place at the right time.

The second objective of a sound maintenance strategy is to facilitate a program of continuous, orderly, incremental change in the operation and, if appropriate, in the basic services provided by the automated system and the business processes it supports. Mission-critical operations now supported are often non-stop public safety processes, such as arrest processing and emergency-response call centers. In these circumstances, 100 percent uptime is a justifiable objective. Downtime associated with major systems changes to achieve technical or functional upgrades can adversely affect an organization's mission.

A program emphasizing incremental, transitional change has several key advantages:

1. **Change Management** — Accomplishing orderly change in a public safety program with a non-stop mission is a challenge. The challenge is even greater when change occurs infrequently and in larger, and perhaps more risk-prone, segments. In an organization geared for incremental and frequent change, the mechanisms of change management are used often and remain viable and responsive. Staff and methods for developing, testing and documenting new systems and procedures — so critical for a successful change program — can sustain a high state of proficiency. Change, and its effective management, should become an integral part of an organization's culture.
2. **Funding Stability** — Government operating budget appropriations are generally decided on a fiscal-year cycle.

Under this commonly used budgeting process, it is usually difficult to obtain significant funding increases from one budget cycle to the next. A system maintenance strategy premised on consecutive years of low-maintenance expenditures followed by a year of substantial expenditures for a major system upgrade runs a significant risk in tight budget periods of missing an upgrade cycle. An organization risks major system failure due to obsolescence. An incremental maintenance program with relatively stable year-to-year budget appropriation requirements is a more sound administrative approach.

3. **Operational Reliability** — A system maintenance and support approach based on more frequent, incremental change produces an overall reliability record superior to a program based on few and infrequent, but often large, changes. While the latter approach may sometimes produce better uptime results, the infrequent outages that result are very often longer in duration and more disruptive in nature than outages associated with more frequent, incremental change.

Design for Maintenance

Establishing a system maintenance strategy to accomplish long-term objectives begins well before a system goes into operation. *Maintenance is a key criteria in the design of a system being developed, and in the selection of a vendor-supplied system.* With the typical life cycle of an automated system lasting from 5 to 7 years, a system's maintenance program will significantly affect the long-term quality of services it delivers. It is not unusual to devote approximately 10 to 15 percent of a system's development cost to annual maintenance. As a result, at least as much will be spent over the life of the system to maintain and modify it as was spent on its development or purchase.

The information technology industry has made great strides in recent years in developing object-oriented programming techniques that make computer programs easier to maintain. The success of object-oriented program development techniques alerted software developers to the value of modular design, discrete and well-defined component interfaces, and interchangeable components. These improvements in computer software architecture are now yielding real benefits through increased reliability of program code and improved long-term program maintenance. The industry is overdue in addressing the need for similar improvements at the systems-integration level. The very same architectural design characteristics that have succeeded in improving the quality of computer program code can be adopted to improve the quality of system integration implementations.

The characteristics of an architectural system approach include modularity, discrete and well-defined system interfaces, and interchangeable components. These characteristics have been successfully employed in other industries for many years. The financial services and health care industries are two good examples of information-intensive service industries with strong similarities to the criminal justice system.

The liquidity of our financial markets and, as a result, the health and prosperity of our economy rely heavily on the responsiveness, reliability and relevance of computerized information systems in the financial services industry. Their durability and strength is due, in no small part, to the architectural framework created for them by an interwoven network of standards, including generally accepted accounting principles and standards, and an array of securities and banking regulations governing financial transactions.

The health care industry, which accounts for about 12 percent of the nation's gross domestic product, is also an information-intensive industry comprised of many thousands of independently managed organizations. It provides one of the best examples of the critical value of reliable, responsive and relevant computerized information systems.

The health care industry has made huge investments in information technology to support the needs of virtually every segment of the industry, including research, delivery of health care, administration of health care institutions, patient records, billing, insurance claims processing and other segments. The daunting task of reliably exchanging electronic information concerning millions of patients among the hundreds of thousands of health care providers, suppliers and insurance companies has been addressed by the industry through an architectural approach. The industrywide

HL/7 Standard includes specifications for data and messaging formats that provide a reliable and efficient means for health care providers and insurers to exchange information on a broad scale.

If the first objective of a criminal justice information system maintenance program is to provide a relevant, reliable and responsive system to support and enhance public safety, we can learn much from the approaches taken by the financial services and health care industries. Valuable software development benefits have been realized in these industries through the use of the rigorous architecture provided by object-oriented programming, and in the application of systems-architecture approaches. We should learn and benefit from these experiences, and build on them. If we address issues affecting long-term maintenance of our criminal justice information systems through an architectural approach from the design phase forward, we will establish a solid foundation for the future development of these systems as the demands placed upon them increase.

Maintaining the Integrated Criminal Justice Information System

So far, we have examined the issues and difficulties of providing and maintaining computerized public safety information systems that are relevant, reliable and responsive. At the same time, maintenance programs designed for these systems must ensure their viability for the long term through a strategy of incremental change. This is a challenging task, even for a stand-alone system. But we now recognize that it is no longer sufficient for individual criminal justice agencies to provide for their own information system needs without also considering, and providing for, the integration of their systems with peer agencies in the community.

Experience in a variety of jurisdictions has taught us that real, tangible benefits are realized by communities where criminal justice agencies work together to improve operations through the use of information technology. The principle underlying this view is that the criminal justice system is a continuum of offender-based processes that operate best when linked together and supported by the smooth flow of information. The traditional approach of treating the system as a series of independent processes often leads to processing bottlenecks as work volumes and other environmental conditions vary. In jurisdictions where the criminal justice systems operate in this manner, paper documents are usually the primary basis for the exchange of information among the processing agencies. Even where agencies have automated their internal case management systems, transferring a case to the next agency in the legal process often involves preparing and submitting case files containing newly completed and signed forms along with abundant copies of supporting case documents.

Costs associated with this labor-intensive approach are substantial, not only for the actual time and material involved but also for the lost opportunities. There are abundant examples of the lost-opportunity cost. One noteworthy example is the time police officers spend participating in lengthy arrest booking procedures. In Baltimore, where more than 80,000 arrests occur each year, it is estimated that the computerized Maryland Arrest Booking System, implemented in November 1995, reduced the time spent by police officers in performing arrest booking procedures by an average of 2 or more hours per arrest. This significant result was achieved through the use of a variety of process improvements, including the use of computer technology to assist police officers in preparing and filing charging documents and completing arrest reports. With less paperwork to do, police officers are returning much sooner to duty in the community. Arrest information is electronically transmitted to the court and detention center computers. Court cases can be opened and offenders can be admitted into pretrial detention or supervision without the need to re-enter information into computer systems. The avoidance of unnecessary paper and the electronic movement of information have provided Baltimore with millions of dollars per year in estimated savings. However, the value of returning police officers to community duty 2 or more hours earlier than before is even greater. The improvements in police officer productivity through the integrated arrest booking system are returning real public safety benefits to Baltimore.

There are other excellent examples where criminal justice agencies have integrated computerized systems to bring about innovative change and real improvements in offender processing and public safety.

SEARCH, The National Consortium for Justice Information and Statistics, conducted research in 1996 and produced a video titled "Integrated Justice Information Systems: Issues, Challenges and Successes" for the Bureau of Justice Assistance. The video identified a number of such success stories, including the Maryland Arrest Booking System, the Midtown Community Court in Manhattan, the Marin County Criminal Justice Information System, and others. The benefits of these various integrated criminal justice system implementations are now documented and well understood. These relatively few, but significant, successes in the use of integrated criminal justice information systems portend an important trend in the nature of criminal justice operations.

Jurisdictions that achieved success in developing and operating integrated criminal justice systems did so using approaches that shared important characteristics. At the same time, the approaches differed in important ways compared to approaches taken to implement individual information systems for criminal justice functions. If the strategy to ensure the long-term viability of computerized information systems begins with the design of the system, let us examine some of the key factors and their potential impact on system viability.

Interagency Coordination

Criminal justice processes are performed by government agencies with defined roles and responsibilities that are usually set out in statute and case law. The responsibilities of most criminal justice functions are defined in their jurisdiction's constitution or charter. The responsibility and authority of criminal justice agency executives are often similarly defined. This arrangement helps provide the appropriate checks and balances to form a justice system based on due process. Another result is the establishment of a justice system comprised of independent agencies with specific functional roles. Recent experiences with integration efforts of criminal justice information systems have shown that the best integration results are achieved when offender processing is viewed as a continuum, rather than as a series of individual processes. Best practice, in this context, refers to providing accurate and complete information in a timely way to support prompt processing of offenders' cases. The vision provided for us is an apparent paradox, where a set of functionally independent organizations must operate a continuous-flow offender processing system in order to succeed. The solution is, of course, to make innovative use of information technology to form the continuous process while maintaining the administrative independence of the participating agencies.

Achieving sustained interagency cooperation and coordination on the scale and for the time frame needed to plan, design, procure and implement an integrated justice information system is not easily accomplished. Each participating agency has operational demands vying for attention, funds and management skills. Changes in laws and regulations, workload increases, and the maintenance requirements of internal systems cause competing pressures for these resources. Moving forward with an integrated criminal justice system in this environment is not an easy accomplishment. This is a vital issue that must be addressed decisively in order for the integrated justice system initiative to succeed.

In the private sector, similar issues are addressed by creating a matrix organization structure reporting relatively high in the company, with a budget allocation, clear mission and stipulated schedule. This approach is also feasible in a government setting. Establishing a similar structure in a government setting is usually accomplished by adoption of a specific law establishing a board or commission and charging it with the appropriate authorities and responsibilities. In some jurisdictions, an executive order or corresponding administrative instrument is sufficient.

Successful interagency coordination is an essential component of implementing and maintaining an integrated justice information system for the long term. Establishing the governance mechanisms to achieve this objective will be discussed in more detail in Section II, *Designing an Integrated System for the Long Term.*

System Compatibility

Criminal justice information systems integration requires the timely interchange of relevant information among agency-operated systems. There are other operational requirements for a successful system, but this particular requirement is notably important. Just as interagency coordination is essential to establishing the integrated criminal justice system as a vital government asset, system compatibility is essential to achieving and sustaining a successful operation.

Compatibility among computer systems in this context means that the various information systems comprising the integrated criminal justice system are capable of reliably transmitting and receiving information to and from each other. The information transmitted must also comply with previously agreed-upon standards on format and content. The first part of this requirement has largely been met. Open systems architectures involving standards-based protocols for communications and information representation are in widespread use in criminal justice information systems. It is in the second part of the requirement where difficulty is almost always encountered.

With a few notable exceptions, there are no generally accepted standards for criminal justice information exchange. One important exception is the work done by the National Institute of Standards and Technology (NIST) to develop a standard for the interchange of fingerprint identification information. This standard will play an essential role in making possible the timely fingerprint identification of criminal offenders on a national scale. Agencies purchasing fingerprint identification systems can now do so with confidence that they will be able to participate in the national fingerprint identification system — the FBI's Integrated Automated Fingerprint Identification System, or IAFIS — provided that the system they purchase complies with the NIST standard.

This is an important fundamental accomplishment. The national exchange of fingerprint identification information will be conducted using an open standard that was developed in a democratic process involving vendors, customers and other stakeholder organizations. Participation in the national system is not tied to a particular vendor solution, but is tied to an information exchange standard that facilitates widespread participation for vendors and their customers, the criminal justice agencies throughout the nation.

The absence of generally accepted standards for the format and content of other criminal justice information poses a difficult and costly problem for jurisdictions planning to integrate their criminal justice information systems. Even those jurisdictions that do succeed in their integration efforts are often left with a maintenance puzzle that rivals the legendary Gordian knot.

Planning and Budgeting

Sustaining the success of a integrated criminal justice information system over the long term relies very heavily on program plans that clearly articulate a multi-year strategy for further development and maintenance of the integrated system. An important role of a program plan is to provide a basis of accountability for budget appropriations requested for implementation of the plan.

It is a customary practice in government organizations to develop program plans for new initiatives to justify requests for additional funds. In consideration of the continuous, incremental change approach to computerized information systems maintenance, a better approach may be to develop and maintain program plans for the system that fully describe the role and benefits achieved through the maintenance program as an integral part of the agency's information technology strategy. This inclusive approach to planning and budgeting provides a comprehensive view to budget officials and legislative bodies that will be helpful in sustaining budgetary support for maintenance operations during tight fiscal periods.

Characteristically, budget appropriations are authorized based on agency-aligned organization structures. This budgeting approach provides for clear lines of authority and responsibility for each agency's performance consistent with their budget appropriation. Program management, procurements, contracts and internal controls all align very clearly with the organization and budget structure. Multi-agency programs, such as the integrated justice information system, are difficult to establish and operate when the allocation and control of resources essential for success are divided among the constituent agencies. It is generally preferable to establish a discrete budgetary program for an integrated justice initiative.

An effective integrated justice information system involves much more than developing mechanisms to transfer information directly among participating agencies to facilitate efficient operations. There are a variety of valuable integrated justice functions that can be effectively provided only where they are established as a resource in common for the participating agencies. Examples include a comprehensive event notification capability, criminal history record information, and a systemwide research and statistical resource. Long-term operational viability of valuable resources such as these is not well secured in a planning and budgeting environment aligned strictly along agency boundaries.

The realities of budgeting politics are such that services provided to other agencies are usually among the first to go when an agency is experiencing funding constraints. Agency-based programs affecting their mission-specific performance will almost always receive funding priorities over multi-agency programs funded internally. A planning and budgeting mechanism is needed that establishes appropriate controls to provide sustained support for multi-agency or enterprise-level integrated criminal justice system resources.

Funding Strategies for the Long Term

Funding patterns for information technology initiatives are often characterized by periodic large requests for funds to provide for major system upgrades or replacements. This can present problems in achieving funding required for major system maintenance or functional enhancements. Budget systems are usually geared toward sustaining a base budget appropriation with some incremental adjustment provided for inflation. As a general rule, expenditures for information technology assets are not considered good candidates for capital budget appropriations. Depreciation patterns of these assets have been relatively short compared to other government assets, and are not always predictable. As a result, the integrated justice system program manager must find a way to flatten annual expenditures for these assets at a level sufficient to provide for their long-term viability.

There are options available to achieve this objective. Although information technology assets, particularly software, are not usually candidates for capitalization, they can often be financed at very competitive rates. For large system expenditures, where the expected useful life of the system is 5 to 7 years, consideration should be given to funding the original procurement through a life-cycle financing agreement. Using this approach, there are at least two viable means to obtain 5- to 7-year financing for a new system. First, the original procurement process can include a requirement for offering vendors to provide the required financing. Second, a simultaneous procurement can be conducted for financing by soliciting proposals directly from financial institutions. Often, the best overall approach is to do both. By requesting vendors to submit system proposals with optional financing while soliciting separate financing options at the same time, an agency can select the combination of system technical value and financing terms most appropriate to its needs.

Using this technique, an agency's annual budget request for the information system would include an annual financing payment amortized over the useful life of the system, and the annual maintenance and support costs. The relatively flat year-to-year budget request facilitated by this technique meets with far less resistance in the budget process than an approach requiring periodic peak appropriations of funds. With the recommended maintenance approach providing for continuous incremental improvements, the base budget may contain sufficient funds at the conclusion of the expected useful life of the system to sustain the enhanced system for a time frame well beyond the original estimate. The alternative is to commence a system upgrade, or replacement if necessary, using the same financing technique to maintain a relatively flat budget appropriation.

The strategy of combining a maintenance program of continuous, incremental improvements with a budgeting strategy based on life-cycle financing can be sustained for the long term. This synchronized approach involving maintenance strategy and funding strategy is an effective means to provide for the long-term viability of information technology assets.

Information Quality Assurance and Security

Maintaining the quality and security of information contained in the integrated criminal justice information system is essential to provide for the long-term success of the system. There is no quicker or more certain way for users to lose confidence in a system than to allow a deterioration in the quality and security of the data it maintains.

Information retrieved from

criminal justice information systems is used at an increasing rate for employment and licensing decisions, as well as for traditional criminal justice purposes. In a criminal justice setting, the safeguards of due process are usually effective in ensuring that offender criminal history record information is available for examination for accuracy by the offender, or by his or her representative, before it is used in a criminal proceeding. Criminal history record information used for employment and licensing purposes is also subject to review and challenge by the subjects of the records. However, harm can occur to the subject of an inaccurate record before the inaccuracy can be corrected in these noncriminal justice situations. Employers in particular will go on to make the best hiring decision from their perspective with information available to them at the time.

Assuring data accuracy is even more difficult in an integrated information system when agencies populate their own computerized records systems with information that originated elsewhere in the criminal justice system that is electronically transmitted to them. If a pattern develops where inaccurate, or even incomplete, information is received by an agency for use in its information system, and the source of the error is not promptly addressed, the receiving agency would be justified in abandoning use of information similarly received.

Ensuring the long-term viability of the integrated criminal justice information system depends upon establishing internal control mechanisms to quickly identify the occurrence of inaccurate information, and initiating timely corrective action. Establishing and administering an appropriate system of internal controls on interagency data exchanges cannot be practically accomplished as an agency-based initiative. An enterprise-level initiative, based on data interchange standards, is the most effective means to achieve success in an integrated justice quality assurance program.

An equally important issue affecting the criminal justice information system integrity is the application of appropriate safeguards to prevent access by unauthorized persons. Considerable improvements have occurred in the availability of control mechanisms to govern access to criminal justice information systems. This is also a matter of internal controls that is most effectively administered at the enterprise level. (The enterprise level is the organizational level where policy is established governing operation of the integrated criminal justice information system, including the flow of information among the participating agencies.)

Implementations of agency-based access control systems are a frequent occurrence because of the inherent responsibility of each agency to protect its information assets. However, a “go-it-alone” approach can quickly lead to a tangle of incompatible security controls that are difficult and expensive to administer, and that can inhibit the authorized sharing of information. An agency-based access control environment can, in the absence of enterprise-level guidelines, substantially limit the effectiveness of an integrated justice system program.

A potentially more significant risk than unauthorized access is the unauthorized use of information by authorized users. This risk is potentially more significant because it cannot be prevented, and is often very difficult to detect. In many cases, the first warning that unauthorized use is being made of criminal justice information is an inquiry or complaint from the subject of a record when they become aware that their record has been accessed and used for an unauthorized purpose. The list of possible uses of criminal justice information for unauthorized purposes is a long one, including illegal activities such as extortion and harassment of the record subject. Mechanisms to determine the source of records used in such an unauthorized manner is an important capability that must be included in the criminal justice information system to ensure that its integrity is not damaged by misuse. In an integrated system environment where information is exchanged electronically, it is vitally important that an enterprise-level audit trail be reliably administered under uniform guidelines developed at the enterprise level.

II. Designing an Integrated System for the Long Term

The importance of a sound and effective maintenance strategy for the long-term success of criminal justice information systems has been described in Section I, *Maintaining Criminal Justice Information Systems.* Two primary objectives were identified. The maintenance strategy must:

1. Deliver value in support of the agency's operational mandate by providing relevant, reliable and responsive information services, and
2. Facilitate a program of continuous, orderly and incremental change to provide sustained improvements in services delivered by the system.

Vital to accomplishing these objectives is a series of factors largely external to the maintenance program. These factors arise for the most part because of the complexities introduced by the multi-agency integration of information systems. In an integrated system, issues that are straightforward in a single-agency system become more complex. Additional issues that must be explicitly addressed at the enterprise level to ensure success in a multi-agency integrated system environment include:

1. Development of program plans for the integrated system;
2. Coordination of multi-agency budget requests and priorities;
3. Information quality assurance and security;
4. Selection of operational priorities;
5. Determination of the integrated system's functions;
6. Determination of data exchange standards and protocols; and
7. Utilization of compatible computer systems and software between agencies.

All of these are *enterprise-level* issues in that they are best managed at the organizational level where policy is established governing operation of the integrated criminal justice information system, including the flow of information among the participating agencies. In addition, Issues 5, 6 and 7 are most effectively resolved within the context of an architectural design for the system. Referring to the discussion in Section I, the characteristics of an architectural design for an integrated justice information system include modularity, discrete and well-defined system interfaces, and interchangeable components. These two concepts, *enterprise-level management* and *architectural design*, are involved so directly in the key issues related to the long-term success of the integrated criminal justice information system that they can be considered critical success factors. A closer examination of these concepts is warranted given their vital role.

Enterprise-level Management

Implementation of integrated criminal justice information systems yields such substantial benefits in operational efficiency to the participating agencies that investments are often fully recovered in a few years. However, there are a variety of powerful reasons to implement these systems that go beyond operational efficiency. In many ways, the quality of justice system operations are substantially improved through the implementation of new information functions provided by the integration of systems. These are, for the most part, not necessarily derived from the direct sharing of information between agencies to support case management processing. These are benefits that derive from new information assets such as databases and communications channels established to meet the common needs of the participating agencies and, in many cases, to meet needs of key external stakeholders. These resources and information assets are defined as enterprise-level assets. Examples include offender identification functions, criminal history record information, event notification functions, and research and statistics information repositories.

Each of these four enterprise-level information assets can provide significant benefits not only to the participating criminal justice agencies; they are also capable of meeting a broad variety of needs well beyond agency case-processing applications. To do so, they must be designed, established and managed at the enterprise level of the criminal justice information system. Several examples include:

1. Timely notification of victims and witnesses upon the occurrence of a variety of offender-specific events;
2. Notification of judges, police investigators and probation officers of criminal justice processing events involving offenders under their jurisdiction; and
3. Research and statistics supporting proposed sentencing laws, and forecasts of arrest and conviction rates related to operating budget and prison construction needs.

There are many other examples of valuable uses of information not specifically related to a particular agency, but involving correlated information from multiple sources. Jurisdictions that have implemented similar enterprise-level information assets have experienced a high level of use.

A commonly used organizational structure to exercise enterprise-level management over the integrated criminal justice information system is a board or commission comprised of senior management representatives from the participating agencies, and of representatives from other organizations with a specific interest in the operation of the system. For example, a state criminal justice information system advisory board (CJIS Advisory Board) often has one or more members from the Legislature, the state Chief Information Officer or his or her representative, and one or more members representing the public in addition to criminal justice members. The public members would usually be representatives of organizations, such as daycare center directors associations, recreation councils and many others involved in the noncriminal justice use of criminal records or other criminal justice information. The broad-based composition of the CJIS Advisory Board helps ensure that the spectrum of interests in criminal justice information is represented. A county or municipal CJIS Advisory Board would not usually be as large, or require such a broad cross section of representation. However, for small and large jurisdictions alike, it is important that the composition of the CJIS Advisory Board be fully representative of the participants and stakeholders of the criminal justice information system.

The best arrangement for establishing a CJIS Advisory Board is through statute or regulation. This is especially important when the information in the system will be used for noncriminal justice purposes. For a local government integrated criminal justice system, it is usually not necessary that the CJIS Advisory Board be established by law or regulation. It is important, however, that the Board be established formally by executive order or by a memorandum of understanding among the participants. In all cases, it is essential that the CJIS Advisory Board's composition, provisions for designating a chairperson, roles, responsibilities, authority and reporting requirements be clearly spelled out in the enabling instrument.

In general, CJIS Advisory Boards do not exercise executive or policy authority over the operation of the criminal justice information system. The Board's authority is usually limited to advising officials responsible for operating the system on matters of policy and data standards, reviewing and preparing legislation and regulations related to criminal justice information, preparing program plans, and exercising reviews of system operations and security through audits.

The CJIS Advisory Board may operate most effectively in a subcommittee structure, particularly in larger jurisdictions where the systems and issues tend to be more complex. A typical structure in a state CJIS Advisory Board could include subcommittees for:

1. Plans and Budgets
2. Policy, Legislation and Regulation
3. Quality Assurance, Audit and Security
4. System Architecture

The System Architecture Subcommittee has responsibility for matters related to functional capability of the integrated system, compatibility of computer systems and software, and standards for information exchange.

Maintenance of the integrated criminal justice system for the long term is a challenging task. These systems tend to be complex because of the dynamic and demanding nature of criminal justice operations. Successfully maintaining these systems for the long term is made even more difficult by additional factors. Continuous changes are occurring in laws and policies affecting the operation of these systems and the information they maintain. In addition, rapidly evolving technology causes computer information systems to become obsolete in ever-shortening periods of time. Establishing a CJIS Advisory Board with broad representation and an appropriate portfolio of responsibility and authority provides a dynamic governance structure that can respond quickly to the evolving environment. It is a critical factor in the long-term success of the integrated criminal justice information system, but it is not sufficient to ensure success. The second critical success factor is a system integration architecture based on modularity, discrete and well-defined system interfaces, and interchangeable components. The following section discusses an approach to achieving an integrated system based on these architectural principles.

Integrated System Architecture

Reference has been made throughout this paper to the importance of applying architectural principles to the design of integrated criminal justice information systems. While it is not within the scope of this paper to deal fully with this subject, it will be useful to discuss the matter from a perspective and level of detail describing its relevance and importance. The purpose of an architectural approach to an integrated criminal justice setting is to achieve the previously mentioned characteristics of an architectural design. They are:

- modularity,
- discrete and well-defined system interfaces, and
- interchangeable components.

It may be possible to achieve an integrated criminal justice information system without giving consideration to these characteristics. This approach can be termed the “ad hoc” integrated system approach, where custom modifications are made as needed to provide for the intersystem exchange of information among a jurisdiction’s criminal justice case processing systems. However, the maintenance effort and costs associated with the long-term support of a system integrated in this ad hoc manner will be very high, and the useful life of the system reasonably could be expected to be less than a criminal justice system integrated using an architectural approach.

An integrated criminal justice information system is usually comprised of a number of individual case processing systems, each serving one or more criminal justice functions. The systems may have been procured or designed at different times, without their integration having been part of the design or procurement specifications. Integration among the various case processing systems is usually designed and implemented as an independent, subsequent initiative. The integration approach can span a broad variety of methods based on the nature of the available technology, the specific integration objectives set out, and any restrictions or limitations that may exist in gaining access to or changing licensed software. The actual techniques for data interchange range from batch file transfers, transaction emulation, remote database access, remote procedure calls, and asynchronous message transfer. The techniques for accomplishing translation of data codes and formats among incompatible systems is just as varied. As a result, integration efforts of criminal justice information systems are, for the most part, one-of-a-kind efforts, providing very little in the way of reusable software or design methods.

A modular interface design, well-defined interfaces and interchangeable components are all-important characteristics of the architectural approach. They will facilitate the reuse of designs and interface techniques. Each step we take in this direction helps to lower interface costs and shorten implementation schedules as intersystem interfaces for criminal justice systems become more standardized. There are three specific components comprising the integration architecture for criminal justice information systems. They are workflow, data and technology.

Component 1: Workflow

This component of the integration architecture is the focal point of the systems integration efforts. The technique of focusing the initial integration design efforts on the workflow characteristics of the participating criminal justice functions slices across organizational boundaries. For example, a workflow analysis of a typical arrest booking process could easily involve five separate agencies. In many jurisdictions, the police, sheriff, prosecutor, public defender, pretrial services and the courts all have a key role to perform within 24 to 48 hours of an arrest. A workflow modeling analysis of an arrest booking process will very quickly reveal integration opportunities of the information systems involved.

Organizing a criminal justice system at a high level into core processes provides the opportunity to set out our approach to the integration architecture in a clear and manageable structure. The following structure comprised of six core processes is useful for that purpose:

1. Crime Reporting and Investigation
2. Arrest
3. Prosecution
4. Adjudication
5. Incarceration
6. Community Supervision

As a general rule, this structure has the useful characteristic that each of the six processes listed is operated by a dominant agency, even though there are usually multiple agencies participating in the process. This characteristic is useful in that the “owner” of a process, or the dominant agency, should take the leadership role in the development of the integration architecture for that particular process.

Using the techniques of workflow analysis, including process modeling methodologies and charts, clearly illustrates the criminal justice processes, the participating organizations and their relationships with the underlying automated information systems. Opportunities for process improvements can be rapidly identified and diagrammed in “To-Be” illustrations complete with appropriate references to integrated information sources and distributions. This approach provides an excellent, cost-effective method to build a reusable library of “best practice” integrated justice system processes and their related information assets.

At the conclusion of the workflow analysis and development of the “To-Be” workflow model, the data flows to accomplish systems integration are readily identifiable. The next logical step in the systems integration process is to develop integration data flow models for those processing points identified in the workflow models where intersystem data exchanges occur.

Component 2: Data

Information formats and code table values usually differ considerably in the automated criminal justice case processing systems found in most jurisdictions with any significant degree of automation. Unless a particularly disciplined effort was made throughout the life cycle of all the major criminal justice information systems in a jurisdiction, there will be a variety of different code values and formats to represent the same information. The individual information systems of the police, detention center, prosecutor, courts, corrections, parole and probation were, in all likelihood, developed or purchased from different vendors at different times. In many circumstances, it is not unusual for systems operated by the same agency, such as a correctional institution system and a probation system, to be incompatible in data formats and codes. It is the purpose of this data modeling component to identify the data to be interchanged at the process integration points, and to specify the means to reconcile the differences in formats and code values.

It is in this area of reconciliation of data formats and code values that considerable effort is made on a system-by-system, case-by-case basis to enable meaningful communication among the various processes of the criminal justice system. In the health care example cited earlier, the HL/7 standard for the interchange of health care information was developed specifically to address this problem. A similar effort to develop standards for the interchange of criminal justice information would yield potentially enormous benefits in the criminal justice field. It would be reasonable to expect that a broadly accepted standard for data exchange would dramatically increase the amount of data sharing, as well as improve the overall cost-benefit basis for investments in criminal justice information systems. In this data interchange standards-based environment, the capability of any jurisdiction to integrate its criminal justice information systems would not be nullified by selection of a particular vendor’s case processing system. Each system could operate internally using proprietary data formats and codes, and communicate with the integrated system using the data interchange standards. Case processing systems could be upgraded, combined or replaced individually. As long as the data interchange standard was incorporated in the new system, the integrated criminal justice system would continue to operate without impact due to incompatible data formats and codes.

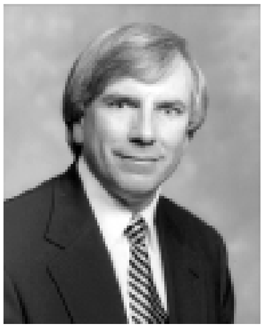
Component 3: Technology

The purpose of this third integration architecture component is to define the means for the interchange of data among the various case processing systems, including the enterprise-level systems, of the integrated criminal justice system. The guidelines for development of a technical architecture for an integrated justice system should focus primarily on the open system building block approach using standards such as TCP/IP, relational database management systems supporting standard SQL, and computer operating systems that implement these standards.

In addition to identifying the basic computing environment infrastructure for the integrated justice system, including the enterprise-level components, the technical architecture must also specify the messaging architecture for the actual transfer of the data being exchanged. The messaging architecture includes specifications on the message triggers, formats, contents, and delivery methodologies for intersystem communications to guarantee successful delivery.

The focus of the integrated criminal justice system technology architecture is on the infrastructure components required to interchange information among the various components of the integrated criminal justice information system, including the enterprise-level components. The technical architecture does not focus on the individual case processing systems, except to specify the technical means for the interchange of data with other components of the integrated system.

The three information system design components — workflow, data and technology — form a comprehensive architectural specification. Integrated criminal justice information systems built on this solid foundation will continue to deliver relevant, reliable and responsive public safety information to the communities they serve for many years.



Criminal Justice Information Privacy

By Robert R. Belair
SEARCH General Counsel
Partner, Mullenholz, Brimsek & Belair

SEARCH General Counsel Robert R. Belair is a partner with the Washington, D.C., law firm of Mullenholz, Brimsek & Belair. Mr. Belair is also CEO of Privacy and Legislative Associates, a legal and policy consulting firm. Privacy and information law involving administrative, legislative and litigation activity are the principal emphases of Mr. Belair's practice. He provides counseling in all aspects of privacy and information law, including educational, criminal, juvenile, medical, employment, credit and financial records; telecommunications; defamation; criminal justice administration; constitutional law; and intellectual property, including software copyrights.

As SEARCH General Counsel, Mr. Belair contributes to SEARCH's privacy and security programs. He authored many studies in criminal justice information law and policy. Mr. Belair was actively involved in revising SEARCH's standards for criminal history record information, Technical Report No. 13: Standards for the Security and Privacy of Criminal History Record Information (Third Edition).

Mr. Belair is former Deputy General Counsel and Acting Counsel for the Domestic Council Committee on the Right of Privacy, Office of the President.

Mr. Belair is a graduate of Kalamazoo College (Michigan) and Columbia University School of Law.

I. The Criminal Justice Information Environment

Several profound developments that may be outflanking established privacy protections for criminal justice information may necessitate a new look at appropriate law and policy for managing this information. Not since the emergence of computers and automated criminal justice information systems in the late 1960s has a combination of technological, political and marketplace developments challenged traditional notions about how criminal justice information should be managed and protected.

In 1967, the Report of the President's Commission on Law Enforcement and the Administration of Justice spoke of the need for an "integrated national information system" and recommended the establishment of a "national law enforcement directory that records an individual's arrests for serious crimes, the disposition of each case and all subsequent formal contacts with criminal justice agencies related to those arrests." The report also emphasized that it is "essential" to identify and protect security and privacy rights in order to assure a credible and politically acceptable national criminal justice information system.[1]

For most of the last 30 years, the U.S. Department of Justice, working through the Federal Bureau of Investigation (FBI), the Law Enforcement Assistance Administration (LEAA) and its successor agencies,[2] has worked toward implementing an automated national system for the exchange of criminal history records, along with a set of comprehensive privacy standards. The following prominent features dominate that environment:

- **Central State Repositories**: Every state established a "central state repository" operated by a state law enforcement agency. Central state repositories maintain a fingerprint record of every individual arrested in the state for a serious/reportable offense (standards vary among the states but, customarily, reportable offenses are misdemeanors punishable by a year or more in prison plus

[1] SEARCH, Technical Report No. 2, "Security and Privacy Considerations in Criminal History Information Systems" (1970) at pp. 3-5 (quoting from the President's Commission Report).

[2] Including, in particular, the Office of Justice Programs (OJP), the Bureau of Justice Statistics (BJS), the Bureau of Justice Assistance (BJA), and the state and local criminal justice information community, including SEARCH, The National Consortium for Justice Information and Statistics, and the FBI's Criminal Justice Information Services Advisory Policy Board (CJIS APB).

felonies). The repository also maintains an automated record of those individuals' arrests along with all available dispositions. This record is referred to as a criminal history record, or "rap sheet."

- **Repository Mission**: The central state repository's principal mission is to provide criminal history record information to state and local law enforcement agencies. The repositories also provide criminal history record information to other components of the criminal justice system — courts, prosecutors and corrections.[3]
- **Liaison With FBI**: Repositories serve as contact points and liaisons with the FBI; send fingerprints and arrest and disposition information to the FBI; respond to search inquiries from the FBI; and initiate search inquiries to the FBI on behalf of authorized, in-state requestors.
- **Criminal Justice Access**: Law and policy in every state provides that criminal justice requestors can obtain all information in a criminal history record unless the information has been sealed by statute or court order.
- **Noncriminal Justice Access**: The repositories provide criminal history record information to noncriminal justice requestors authorized by state law, such as licensing boards and certain types of employers. In most states, authorized noncriminal justice requestors receive less than the full record — most often limited to conviction-only information.
- **Public Access**: Except in a few "open record" states, the general public is not authorized to obtain criminal history record information from the central state repository.
- **Record Subject Access**: In virtually every state, record subjects are entitled to obtain access to, and have the right to correct, criminal history record information maintained by the repository which relates to them.
- **Fingerprint and Name-Only Access**: In virtually every state, all criminal histories maintained by a central state repository must be supported by a fingerprint record and, with certain exceptions, requests for criminal history information must be accompanied by a fingerprint. Fingerprint support insures that the record maintained at the repository relates to the correct person, and that the repository's response relates to the correct person. The principal exception is for law enforcement requests in instances during which the law enforcement agency does not have the individual in custody and, therefore, cannot provide a fingerprint, or in situations requiring quick turnaround. In those instances, a "name-only" check (customarily including a name, gender, date of birth, race and other physical indicators) is permitted.
- **Information Maintained by Repositories**: Traditionally, central state repositories maintain subject identification information (fingerprint records), criminal history information and certain other information, such as pretrial release information and felony conviction flags. Repositories virtually never maintain other types of personal information, such as employment history, medical history, military or citizenship status.[4]
- **Content of Criminal History Record Information**: Historically and traditionally, criminal history record information consists of identifying information, arrests and available dispositions, but little or no information about third parties such as witnesses, victims or family members.[5]
- **Disposition Reporting**: Repositories attempt to obtain disposition information from the courts and, in recent years, the percentage of arrests maintained at the repositories that include available dispositions has increased substantially.
- **Juvenile Justice Information**: Customarily, repositories do not maintain juvenile justice information. Those few repositories that do maintain juvenile justice information do not integrate it with any adult record the individual

[3] For a detailed discussion of the uses of criminal history records by law enforcement, courts, prosecutors and corrections, *see*, SEARCH/Bureau of Justice Statistics, "Use and Management of Criminal History Record Information: A Comprehensive Report" (1993) at pp. 14-17 [hereafter, "Use and Management of Criminal History Record Information"].

[4] Ibid., at pp. 22-23.

[5] *See*, SEARCH/Bureau of Justice Statistics, "Increasing the Utility of the Criminal History Record: Report of the National Task Force" (1995) at pp. 23-27.

may have. (As a practical matter, juvenile justice information, until very recently, was not available on any kind of reliable or organized basis. Rather, each separate juvenile or family court and each separate law enforcement agency would maintain juvenile records. These records frequently were not automated or fingerprint-supported. Moreover, some of these records were not available by law (based on sealing requirements), even to criminal justice agencies until recently.)

- **Investigative and Intelligence Information**: Investigative and intelligence information is almost never maintained at a central state repository. When it is maintained, it is never integrated with criminal history record information. More frequently, investigative and intelligence information is maintained only at the local police agency or law enforcement agency level. It is not automated or fingerprint-supported, and is only shared on a closely held, need-to-know basis within the law enforcement community.[6]
- **Original Records of Entry**: Pieces of an individual's criminal history record — but only infrequently an individual's entire criminal history record— are held in "open record" files maintained by police agencies and by the courts. These original records of entry describe formal detentions and arrests and include incident reports, arrest reports, case reports and other documents which are constitutionally mandated to be publicly available, and which document that an individual has been detained, taken into custody or otherwise formally charged. In addition, records of court proceedings maintained by the courts include indictments, arraignments, preliminary hearings, pretrial release hearings and other court events that, by law and tradition, are open to public inspection. Until very recently, both types of open-record systems were manual or only partially automated at best, were not comprehensive or reliable, and related only to events occurring at the particular law enforcement agency or court. As a consequence, these systems were difficult and expensive to use, and were largely unsuitable for compiling a reliable or comprehensive criminal history record file.
- **FBI Role**: At the federal level, the FBI functions as a criminal history repository holding both federal offender information and records of arrest and dispositions under state law.
- **Interstate Identification Index** (III): During the last 30 years, the FBI has worked with the state criminal justice information community to develop the III. When completed, III will permit authorized requestors to access an FBI-maintained index supported by a National Fingerprint File (NFF) in order to determine whether any state (or the FBI for federal offenses) maintains a criminal history record about a particular subject.
- **III Compact**: In October 1998, Congress enacted S. 2022, which includes the National Crime Prevention and Privacy Compact Act (III Compact). Once ratified by the states, the III Compact will permit III to be used by authorized, noncriminal justice requestors. At that point, the FBI will cease to obtain arrests and dispositions relating to state offenses and the national system will operate through the FBI III index and the NFF.
- **Local Agency Role**: During this same 30-year period, local agencies, with the rare exception of the very largest local agencies, have withdrawn from the business of maintaining formal and comprehensive criminal history records other than booking information and other original records of entry. Instead, local agencies rely on the state repository and, through the state repository, the FBI to provide complete and comprehensive criminal history records.

II. Criminal Justice Privacy Standards

Privacy standards for criminal justice information received considerable attention beginning in the late 1960s and extending throughout the 1970s. However, these privacy protections were not then and are not now driven by constitutional considerations.

[6] *See*, SEARCH/Bureau of Justice Statistics, "Criminal Justice Information Policy: Intelligence and Investigative Records" (1985) at pp. 43-49.

A. Constitutional and Common Law Standards

The Constitution remains largely neutral with respect to the privacy of criminal history record information. In particular, the U.S. Supreme Court has held that the Constitution does not recognize a privacy interest in the dissemination by criminal justice agencies of information about official acts, such as arrests.[7] In 1989, the Supreme Court did recognize that there is a statutory privacy interest, under the Federal Freedom of Information Act,[8] in automated, comprehensive criminal history records. It is unlikely, however, that the Court will extend this statutory interest to reach the constitutional right of information privacy, which is tentative and nascent at best.

In 1995, the Court again addressed the privacy threat posed by computerized criminal history information. In *Arizona v. Evans*,[9] the Court found that the "exclusionary rule" does not require suppression of evidence seized incident to an arrest resulting from an inaccurate computer record when the error was caused by court, rather than police, personnel. In a concurring opinion, Justice Sandra Day O'Conner noted that with "the advent of powerful, computer-based record keeping systems that facilitate arrests in ways that have never before been possible. The police … are entitled to enjoy the substantial advantages this technology confers. They may not, however, rely on it blindly. With the benefits of more efficient law enforcement mechanisms comes the burden of corresponding constitutional responsibilities."[10] Justice Ruth Bader Ginsburg, in dissent, also expressed concern over the impact of modern technology on privacy: "Widespread reliance on computers to store and convey information generates, along with manifold benefits, new possibilities of error, due to both computer malfunctions and operator mistakes …. [C]omputerization greatly amplifies an error's effect, and correspondingly intensifies the need for prompt correction; for inaccurate data can infect not only one agency, but the many agencies that share access to the database."[11]

Furthermore, common law privacy doctrines, such as the widely recognized privacy tort of public disclosure of private facts, have proven ineffectual when applied to criminal history record information. Sovereign immunity, civil and official immunity, and the need to show tangible harm arising from the alleged disclosure or misuse of criminal history records have proven to be virtually insurmountable obstacles to common law privacy actions.[12]

B. Federal Criminal History Record Legislation and Regulations

Privacy standards for criminal history information have been left largely to statutory and regulatory initiative. During the 1970s, when public concern about privacy, automation and governmental and private information systems was running high, the Congress considered several legislative proposals that would have imposed uniform, national information and privacy standards for criminal history record information. All of those proposals failed.[13]

In 1973, however, the Congress did enact as an amendment to the Omnibus Crime Control and Safe Streets Act of 1968 the so-called "Kennedy Amendment," which provided that all criminal history record information collected, maintained or disseminated by state and local criminal justice agencies with financial support under the Omnibus Crime Control and Safe Streets Act must be made available for review and challenge by record subjects and must be used only for law enforcement and other lawful purposes.[14] LEAA implemented the Kennedy

[7] *Paul v. Davis*, 424 U.S. 693, 713 (1976).

[8] *Department of Justice v. Reporters Committee for Freedom of the Press*, 489 U.S. 749 (1989).

[9] 514 U.S. 1 (1995).

[10] Ibid., at 17-18 (O'Connor, J., concurring).

[11] Ibid., at 26 (Ginsburg, J. dissenting).

[12] *See*, a discussion of cases cited at SEARCH, Technical Memorandum No. 12: Criminal Justice Information Perspective on Liabilities (1977) (and as updated in 1981) at pp. 5-20.

[13] *See*, "Use and Management of Criminal History Record Information" at p. 36, supra note 3. The FBI's basic statutory authority to maintain and disseminate criminal history records is at 28 U.S.C. § 534. This provision authorizes the Attorney General to, "acquire, collect, classify and preserve criminal identification, crime and other records" and to, "exchange such records and information with and for the official use of, authorized officials of the federal government, the States, cities and penal and other institutions."

[14] 42 U.S.C. § 3789G(b), as amended by Section 524(b) of the Crime Control Act of 1973, Pub. L. No. 93-83 (1973).

Amendment by adopting comprehensive regulations which set relatively detailed and ambitious standards for data quality (completeness, accuracy and timeliness) but which gave states wide discretion to set their own standards for dissemination.

C. SEARCH Technical Report No. 13

SEARCH has also been active in the formulation of standards for the security and privacy of criminal history record information. Beginning in 1970, the year after SEARCH was established, SEARCH published a series of publications addressing privacy and security in computerized criminal history files, and providing guidance for legislative and regulatory protections for criminal history information.[15]

In 1975, SEARCH published the widely influential "Technical Report No. 13," SEARCH's first comprehensive statement of 25 recommendations for safeguarding the security and privacy of criminal history information.[16] These recommendations influenced LEAA's development of the federal regulations discussed above, and the Appendix to the federal regulations refers states to "Technical Report No. 13" for guidance in formulating their state plans.[17] "Technical Report No. 13" has been revised twice since 1975 (most recently in 1988) to reflect technological and societal changes that have had an impact on criminal justice information management and privacy.[18]

D. State Legislation

Throughout the 1970s and into the 1980s, states adopted statutes based in large measure on the SEARCH recommendations and the LEAA regulations. By the early 1990s, approximately one-half of the states had enacted comprehensive, criminal history record legislation, and every state had enacted statutes that address at least some aspects of criminal history records. The majority of state laws followed the scheme in the federal regulations, which distinguishes between information referring to convictions and current arrests (arrests that are no older than one year and which do not yet have the disposition) and "nonconviction data," which are arrests more than one year old without a disposition or arrests with dispositions favorable to the accused.

Under the federal regulations and many state laws, conviction information can be made available largely without restriction. Nonconviction data, on the other hand, cannot be made available under the federal regulations unless authorized by a state statute, ordinance, executive order or court rule.[19] Furthermore, the federal regulations provide that, when criminal history information is disseminated to noncriminal justice agencies, its use "shall be limited to the purpose for which it was given."[20]

E. Current Approach to Protecting Criminal Justice Record Privacy

Today, a relatively stable and uniform approach to protect the privacy of criminal justice information is in place throughout the United States. Five fundamental principles characterize the U.S. approach to protecting the privacy of criminal history record information:[21]

- **Restrictions on the Collection and/or Integration of Criminal History Information**: Most states have adopted formal or informal restrictions to segregate criminal history record information from other types of personal information. Thus, criminal history record information seldom contains juvenile justice information; virtually never contains investigative or intelligence information; and virtually never contains medical, employment, financial, military or citizenship status information, or other types of personal information.
- **Data Quality and Data Maintenance Safeguards**: As of 1997, all 52 jurisdictions

[15] *See*, SEARCH, Technical Report No. 2, "Security and Privacy Considerations in Criminal History Information Systems" (1970); Technical Memorandum No. 3, "A Model State Act for Criminal Offender Record Information" (1971); and Technical Memorandum No. 4, "Model Administrative Regulations for Criminal Offender Record Information" (1972).

[16] *See*, SEARCH, Technical Report No. 13, "Standards for the Security and Privacy of Criminal Justice Information" (1975).

[17] *See*, 28 C.F.R. Part 20, Appendix § 20.22(a).

[18] SEARCH, Technical Report No. 13 (Revised), "Standards for the Security and Privacy of Criminal History Record Information" (3rd ed.) (1988). The second revision occurred in 1977, at which time the commentary to the 1975 report was expanded, but the original recommendations were unchanged. Ibid., at p. 1.

[19] 28 C.F.R. § 20.21(b).

[20] 28 C.F.R. § 20.21(c)(1).

[21] *See*, SEARCH/Bureau of Justice Statistics, "Compendium of State Privacy and Security Legislation: 1997 Overview" (1998) at pp. 4-11.

surveyed by SEARCH on a biennial basis (the 50 states plus Puerto Rico and the District of Columbia) had adopted standards to assure the accuracy and completeness of criminal history record information. In addition, 40 states had adopted laws permitting the purging (destruction) of nonconviction information, and 26 jurisdictions had adopted standards for purging conviction information if certain conditions are met. As well, 31 states had adopted laws and regulations to permit the sealing of nonconviction information, and 30 states had adopted laws and standards to permit the sealing of conviction information.[22]

- **Subject Access and Correction**: As of 1997, 51 jurisdictions give record subjects a right to inspect their criminal history records, and 45 jurisdictions permit record subjects to challenge and/or offer corrections for information in their criminal history records.
- **Security**: As of 1997, 43 jurisdictions had adopted formal standards for technical, administrative, physical and/or personnel security. As a practical matter, however, security standards are in place for all 52 jurisdictions that have established central state repositories. The extent and nature of those standards vary substantially, however.
- **Use and Disclosure**: As of 1997, all 52 jurisdictions had adopted laws or regulations setting standards for the use and/or dissemination of criminal history record information. As a practical matter, every state makes all criminal history information available for criminal justice purposes. However, while conviction information is widely available outside the criminal justice system, nonconviction information remains largely unavailable or available only to certain types of users, such as licensing boards and certain kinds of employers that employ individuals in highly sensitive positions such as school bus drivers or child-care workers. (Of course, sealing and purging provisions also work effectively to provide dissemination and confidentiality safeguards.)

III. Trends and Change Drivers

By the late 1990s, six relatively distinct and important developments appear to be outflanking the generation of privacy and information safeguards that emerged in the 1970s and the 1980s. These developments are:

- **Technological Change**: Revolutionary improvements in information, identification and communications technologies, including Internet-based technologies.
- **System Integration**: Accelerating initiatives to integrate criminal justice information systems operated by law enforcement, courts, prosecution and corrections, as well as to integrate these systems with information systems maintaining other types of personal information.
- **Noncriminal Justice Demand**: A persistent and ever-increasing demand by noncriminal justice users to obtain criminal history record information.
- **Commercial Compilation and Sale**: Changes in the information marketplace which feature the private sector's acquisition, compilation and sale of criminal justice information obtained from police- and court-based open record systems.
- **Federal Initiatives**: A host of new and well-intended federal initiatives aimed at providing criminal justice information to broader audiences on a more cost-effective and timely basis.
- **Juvenile Justice Reform**: A new paradigm for juvenile justice records, which posits treating juvenile information in a way that very much resembles the handling of adult records.

These developments are taking place against a backdrop of unprecedented interest in and concern about information privacy across the whole spectrum of personal information and record keeping systems.

Technology

Computers have been used to capture and manage criminal justice record information since at least the late 1960s. Until very recently, however, computerized criminal justice record information systems merely created what amounted to an automated "file cabinet." Whoever owned the automated file cabinet had

[22] Ibid., at p. 15.

responsibility for managing the system and, as a practical matter, enjoyed substantial discretion in setting rules for the collection, retention, use and disclosure of information maintained in that automated file cabinet. Today's powerful and nimble information systems facilitate a far different environment. Users can access criminal justice record information and other personal information from any location, and from multiple databases. In doing so, users can create their own multi-dimensional, cross-sectoral, customized, personal information profiles. Today, who maintains these databases is no longer as important as who assembles and draws information from the various databases and the type of customized, comprehensive information product they create.

Changes in information technology permit users to build powerful, customized, personal profiles containing a mix of criminal justice record and noncriminal justice record information. These profiles lend themselves not only to important criminal justice applications, but also to point-of-sale and other noncriminal justice applications.

This information management revolution is occurring contemporaneously with a revolution in identification technology — DNA, live-scan, Automated Fingerprint Identification Systems (AFIS) — giving users the potential not only for a richer, customized information product, but also a product that has a much higher degree of reliability and integrity (that is, an assurance that the information truly does relate to the person who is the intended subject of the inquiry).

The Internet is, perhaps, the final piece of the puzzle — a dramatic and new feature on the information landscape. The Internet is an inexpensive and relatively user-friendly technology; it not only provides robust information management capabilities, but also does so on a real-time, communications platform. Furthermore, the Internet creates remarkable opportunities for national and international publication — and offers remarkable opportunities to threaten privacy. Recently, several states have placed all or parts of their sexual offender databases on the 'Net. A few states are even considering proposals to place some criminal histories on the Internet.

These information technology advances hold enormous promise for criminal justice users and for authorized, noncriminal justice users to obtain comprehensive, reliable and customized information about individuals on a near-instantaneous basis. However, these advances also create or, at a minimum, exacerbate privacy threats. The on-line availability of an individual's criminal history and criminal justice record information — along with the potential to obtain his or her juvenile justice records and information on his or her educational background, financial status, medical history, and immigration and citizenship status — is certain to ignite a new privacy debate about who should get access to this kind of information technology, for what purposes, and subject to what privacy safeguards and restrictions.

Integration

Criminal justice information integration initiatives are accelerating across the nation and are creating criminal justice information systems which pool personal information about an individual from law enforcement, the courts, corrections and prosecution. Integration can also take other forms. Some jurisdictions are integrating across jurisdictions, so that agencies in different local jurisdictions are building integrated systems which serve agencies in numerous, different jurisdictions. Other jurisdictions are integrating local systems with state systems.

Integration is also taking place based on shared technology. For example, many jurisdictions have come together to share AFIS technology, both in an effort to reduce cost and to broaden the database against which searches occur. Some jurisdictions are even integrating criminal justice and noncriminal justice databases. Courts and social service agencies, for example, are building integrated systems containing both criminal justice and social service data. The result is a more comprehensive, timely and accurate product with important benefits for both criminal justice and noncriminal justice users. However, integrated systems create new privacy threats and are expected to be another factor focusing renewed attention on privacy issues.

Noncriminal Justice Demand for Criminal History Record Information

Beginning in the late 1970s, as crime rates rose and as recidivism rates persisted, the American public grew increasingly interested in capturing, maintaining and sharing criminal justice and criminal history record information, and grew less interested in assuring privacy rights and safeguards for arrestees and offenders. During this same period, as noted earlier, the U.S. Supreme Court found that information about arrests and convictions relates to public events and is, therefore, not subject to constitutional privacy protections. The result, throughout the 1980s and 1990s, has been a steady erosion of statutory and regulatory criminal history record information confidentiality and privacy protections.

Today, criminal justice and criminal history record information is available from state central repositories, not just for criminal justice purposes, but also for a wide variety of noncriminal justice purposes. In particular, these purposes include employment background screening, licensing eligibility checks and a wide array of noncriminal justice, governmental purposes. Demand continues to grow. It is a rare legislative cycle that does not see the enactment of new state laws authorizing access to criminal history information for noncriminal justice purposes. In the last Congress, the Senate held hearings on the need for access to criminal history data for nursing home workers; Congress enacted legislation strengthening the National Child Protection Act, which authorizes background checks for employees providing services to children, the elderly and the handicapped; and Congress amended the Fair Credit Reporting Act to permit consumer reports to include conviction information, regardless of how long ago the conviction occurred.

The FBI has just reported that the number of criminal history record access requests that it receives from noncriminal justice requestors now exceeds the number of requests from criminal justice.

Information Marketplace

In the last few years, a new marketplace has emerged to meet the burgeoning demand for criminal history data and to take advantage of changes in information technology. Today, private companies routinely “harvest” arrest and conviction information from newly automated court dockets and, to a lesser extent, from police blotter systems. These companies then sell the criminal history profiles to employers, insurers and other noncriminal justice users. Ironically, the largest single user category for many of these suppliers is government agencies. Further, these companies or their customers often merge criminal record information with an individual’s education, financial, medical and other records, as well as with psycho-demographic data, to create informal but, nonetheless, powerful and comprehensive, information profiles.

Federal Initiatives

The federal government is spearheading numerous initiatives aimed at providing authorized users with better and more timely criminal justice information. The government’s purposes are positive and important, but one inevitable effect is to create at least the potential for new and significant privacy threats. This report describes several initiatives.

Perhaps the most important of the new federal initiatives is the National Instant Criminal Background System (NICS), which became operational as of November 30, 1998. NICS will provide firearms dealers with instantaneous information about whether an individual has a criminal background that makes the individual ineligible to obtain a firearm. NICS will combine criminal history record information with certain other kinds of sensitive information, including medical information and citizenship status, raising the possibility of a comprehensive, automated and federally controlled profiling system. The sensitivity and breadth of this information, combined with its availability on a point-of-sale basis and on a name-only basis, seems certain to add fuel to the criminal justice privacy debate.

Juvenile Justice

The frequency of juvenile crime, its violence and its pattern of persistent recidivism, have combined to generate pressure to open juvenile records to greater use within both the criminal justice and the noncriminal justice communities. Concomitantly, these same forces have generated pressure to improve the quality of juvenile history records, including making the records fingerprint-supported and assuring appropriate disposition reporting. Recent federal legislation (H.R. 3, H.R. 1888 and S. 10) has focused attention on privacy issues associated with juvenile records by including initiatives to rework the juvenile justice information system to make it look much more like the adult system. The effort to improve juvenile history records and to make juvenile history records more available is controversial and adds to the emerging debate over privacy and criminal justice.

IV. Information Privacy Concerns at a Historic High Level

These six trends and “change drivers” are unfolding against a backdrop of extraordinary concern about information privacy. Indeed, as of the late 1990s, information privacy is attracting unprecedented attention and emphasis.

For example, the 105th Congress, which adjourned in October 1998, considered more than 100 privacy bills and devoted almost 50 days of hearings to the issue. In recent years, the Congress has given serious consideration to (and enacted, in some cases) information privacy legislation addressing telecommunications, financial, credit reporting, medical and genetic records, online and Internet information, children’s privacy, government-held personal information (IRS privacy), drivers and motor vehicle record information, and look-up service records (for example, Social Security Numbers and other personal identifiers).

State legislatures have been equally active. In the last legislative cycle, state legislatures considered more than 1,000 information privacy bills and enacted more than 50 important information privacy statutes. These information privacy bills and statutes focused on the same record keeping and information areas as did the federal legislation, with the important addition of insurance records.

At the same time, the federal executive branch has launched numerous privacy protection initiatives. The Federal Trade Commission, the Federal Communications Commission, the Department of Health and Human Services, the Office of Management and Budget, the Office of the Vice President, the federal bank regulatory agencies, the National Highway Transportation and Safety Administration (on intelligent vehicle-tracking systems) and the Department of Commerce have all published privacy-related regulations or guidelines; conducted privacy studies; initiated privacy-related, administrative actions; and/or promoted information privacy initiatives.

In the last few years, privacy has also had a global emphasis. In 1995, the European Union (EU) adopted its Data Privacy Directive, requiring that all 15 EU nations adopt comprehensive and strong privacy legislation and forbidding the transfer of personal information about European nationals to any country which has not adopted “adequate” privacy protections. The Europeans do not believe the U.S. privacy protection scheme is “adequate.” Therefore, the impact of the EU Directive, effective October 25, 1998, has been a matter of grave controversy and concern.

During this period, the media and privacy advocacy groups have sought to direct public attention to what they perceive as the inadequacy of U.S. information privacy protections. A number of companies and industries have been “caught” in privacy violations or privacy crises that have attracted media, advocacy group and, oftentimes, congressional and state legislative attention. In the winter of 1998, for example, a regional drug store chain was forced to abandon plans to share its customer prescription drug information with third parties for marketing purposes after a barrage of print and broadcast media criticism.

As a result of the pressure generated by media, advocacy group and legislative and international scrutiny, and because consumers increasingly expect companies to provide adequate privacy, the private sector has launched an unprecedented effort to develop and implement voluntary privacy guidelines. For example, the Online Privacy Alliance has developed comprehensive, cross-sectoral privacy guidelines for companies that obtain personal information about consumers arising from on-line and e-commerce activity. BBBOnline and TRUSTe are developing a privacy “seal of good housekeeping” with verification and dispute resolution processes. The U.S. Department of Commerce adopted a self-regulatory approach in its November 1998 “International Safe Harbor Privacy Principles,” which are designed to serve as a voluntary framework for U.S. companies to use in order to comply with the E.U. Directive.

These and other self-regulatory programs require or encourage companies to notify consumers about a company’s information and privacy practices; to provide them with a degree of choice in how much information, if any, they wish to make available; and to inform consumers about access and correction rights, data quality protections, security protections and confidentiality safeguards.

Increasingly, these voluntary programs also provide for verification of company compliance and some type of remedy for consumers who are aggrieved by a violation of these self-regulatory guidelines.

These developments set the stage for a re-evaluation of the privacy protections that apply to criminal justice records and criminal justice information systems.

V. Key Public Policy Issues and Questions

Recent trends and "change drivers," as well as the increased interest in information privacy at both the federal and state levels, suggest that there may be a need to re-evaluate current privacy protections provided to criminal justice information. Among the issues to be addressed include:

Issue No. 1: *Should there be restrictions on the type of criminal justice record information collected or compiled or restrictions on its amalgamation with other types of personal information?*

- As a matter of law and custom, criminal history record information has been limited to subject identification information; a history of arrests and dispositions; and, occasionally, other types of information, such as juvenile record information, special felony conviction flags, or pretrial release information.
- The law in more than a dozen states restricts criminal history record information from being integrated or combined with intelligence and investigative information. Even more states have adopted laws or standards that prohibit combining criminal history record information with juvenile record information.
- In recent years, a number of studies and reports have called for expanding criminal history records to include information about victims, witnesses and about certain other third parties.
- The U.S. approach to privacy protection is less apt to restrict collection and amalgamation, and more apt to allow the information to be collected and consolidated, and then to prescribe privacy protections based on use or disclosure.
- Increasingly, end users are capable of drawing various pieces of personal information from different sources and putting together their own customized, personal information profiles. This being the case, does it make sense to restrict the collection of information or the amalgamation of information in criminal history records?

Issue No. 2: *Should there be restrictions on the method (name-only versus fingerprint-based requests) by which criminal history record information is accessed or obtained?*

- Name-only requests are less expensive to process, more convenient and provide faster turnaround. Therefore, even if a fingerprint-supported request provides a more reliable result, should not users be able to decide how to balance the benefits of a name-only check versus their tolerance for the risks associated with this kind of check?
- Changes in technology (live-scan and AFIS) may soon make fingerprinting just as quick, convenient and inexpensive as name-only checks. This being the case, does it make any sense to abandon or limit fingerprinting, just on the verge of a technological remedy?
- If name-only checks begin to supplant fingerprint-based checks, will this have an adverse impact on the size of fingerprint databases available to support AFIS and latent (crime scene) searches?
- Do most noncriminal justice requestors require the kind of quick turnaround made possible by name-only checks?
- Relying on name-only checks will inevitably mean that requestors must collect and use more demographics, such as Social Security Numbers. Does this carry its own privacy risk and provide a further argument in favor of fingerprinting?
- Mismatched information (applying a criminal history record information to the wrong person) is a major privacy threat and is associated with name-only checks. Does this provide a basis for insisting upon the use of fingerprinting?
- The use of aliases and the failure of name-only checks to retrieve available criminal histories increases the possibility of false-negative findings during background checks and can create a public safety threat. Does this threat warrant insisting upon fingerprint-based requests?

Issue No. 3: *Are current sealing and purging policies viable and, if not, how should they be changed?*

- At present, laws in 40 states provide for the purging of nonconviction information, and in 26 states for the purging of conviction information. Also, present laws in 31 states provide for the sealing of nonconviction information, and in 30 states for the sealing of conviction information. The standards for a purge or seal order vary substantially among the states but turn on the type of offense, the number of previous offenses and the establishment of a clean-record period. The methods for obtaining a seal or purge order also vary substantially among the states, and include statutory or automatic sealing or purging mechanisms, as well as record subject-initiated and court-ordered purging and sealing.
- In an era of automated court records and police blotters, automated newspaper morgues and automated commercial criminal history repositories, is it advisable, or even feasible, to permit the sealing or purging of an official criminal history record?
- Should sealing or purging standards apply not just to criminal history records at the central state repository, but also to original records of entry and to privately maintained criminal history record information?
- Should the criteria for a seal or a purge be re-examined and limited?

Issue No. 4: *Should record subject fair information practice/ privacy rights for criminal justice record information be enhanced?*

- Increasingly, notice is a fundamental part of every information privacy law and standard. Does it make sense to mandate notice rights for criminal justice offenders?
- Can it be argued that notice rights are irrelevant to criminal record subjects because they are involuntary participants in the system and, therefore, any notice of privacy rights and information handling practices will not affect their behavior?
- Can it be argued that a notice of privacy rights is trivial, given that record subjects are concerned with grave problems of arrest, pending prosecution and possible incarceration?
- Consent/choice is also a fundamental part of every recent privacy law or standard. Should consent/choice play any role in criminal history record information dissemination policy?
- Given that a criminal history record is inevitably thought of as a pejorative, is it a virtual certainty that every record subject will exercise consent/ choice rights to restrict dissemination?
- Does it make more sense to continue the current policy of prohibiting, as a matter of law, certain types of disclosures, rather than basing disclosures on the exercise of a record subject's choice?
- Should consent/choice play a role in certain types of disclosures, such as disclosures for nonconviction purposes?
- Should criminal justice agencies be required to create and maintain transaction logs indicating when and to whom criminal justice record information is disseminated?
- At present, laws in 43 states require these transaction logs and require that record subjects be given access to the logs. Do these laws provide a significant privacy benefit for record subjects?
- Are the logs a burden for record keepers?
- Should courts and other agencies holding original records of entry also be required to maintain transaction logs?
- Should commercial providers of criminal history record information be required to maintain these logs?
- Should the remedies for violation of criminal justice information privacy standards be reformed? Because of EU pressure, American policy makers have recently taken a new look at the availability and practicality of remedies for violation of privacy law and regulations. Most states provide for both civil remedies and criminal penalties in the event of a violation of their criminal history record statutes. It is not clear, however, whether these remedies are practicable or convenient for record subjects. Furthermore, there is reason to believe that these remedies are seldom invoked.

Issue No. 5: *Should privacy restrictions or safeguards be placed on efforts to integrate criminal justice information systems?*

- Is integration such an important and positive goal that privacy threats that arise from it are so outweighed by its benefits that the privacy threat should be overlooked?
- Are privacy threats posed by integration the type that can be adequately addressed by safeguards on the use or redisclosure of criminal justice record information in integrated systems and, therefore, need not impose any obstacle to the creation of integrated systems?
- Are there certain kinds of integration initiatives that pose more of a privacy threat than other types?
- Are there some types of integration, such as integrating criminal history record systems with intelligence and investigative systems or integrating criminal history record systems with systems containing medical, financial or other very sensitive personal information, that should be avoided or restricted on privacy grounds?

Issue No. 6: *Does the commercialization of criminal history record information through the acquisition of court information and other original record of entry information by private entrepreneurs and its amalgamation with other types of personal information and its redisclosure and sale pose a privacy threat and, if so, can or should anything be done about this threat?*

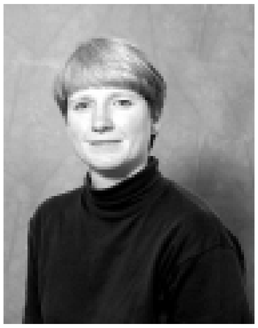
- Does the threat arise from the broader dissemination of commercial criminal history record information?
- Does the threat arise from the danger of matching commercial criminal history record information with the wrong person?
- Does the threat arise from the likelihood that commercial criminal history record information may be less accurate, complete or timely than the official criminal history record maintained in a state central repository?
- Does the threat arise from the claim that commercial compilers and resellers of criminal history record information are likely to be less prudent in their handling of the information or, in any event, are less accountable than are governmental agencies, including state central repositories?
- Does the threat arise from the permanent availability of commercial criminal history record information, thus outflanking sealing and purging standards?
- Does the threat arise from the likelihood of combining commercial criminal history record information with other types of personal information to create a comprehensive and sensitive individual profile?
- Are the purposes for which commercial criminal history record information is used so important and beneficial that they outweigh any privacy threat?
- Do regulatory privacy protections applicable to commercial criminal history record information, such as the Fair Credit Reporting Act and state credit reporting laws, as well as self-regulatory protections, such as those imposed by the Individual Reference Services Group, provide sufficient and appropriate privacy protection?
- Does the First Amendment or other constitutional or public policy values effectively foreclose any restrictions on access to open record and public record, criminal history record information by commercial compilers and resellers?
- Should criminal history record information at a state central repository be fully open to the public on the theory that the information is available to the public through commercial compilers and resellers and, therefore, it makes more sense and provides more privacy protection for the public to obtain the official and more accurate and reliable version of CHRI?

Issue No. 7: *In light of new technologies and marketplace changes, should there be restrictions on the dissemination of criminal history record information and would any such restrictions be viable?*

- Should the source of the criminal history record information or criminal justice record information be a criterion in imposing restrictions? If the source is a central repository, should this suggest more or less restrictions than those placed on a commercial source?
- Should the type of criminal history information or crimi-

nal justice information be a criterion in imposing restrictions?

- Should juvenile justice record information be treated differently than adult criminal history record information?
- Should intelligence and investigative information be treated differently?
- Should witness and victim information be treated differently?
- Should the traditional distinction in information and privacy policy between conviction information and nonconviction information be retained?
- Should the purpose of the intended use be a criterion for imposing restrictions?
- Should the traditional distinction between criminal justice uses and noncriminal justice uses be retained?
- Should there be any distinctions among criminal justice uses?
- Should governmental, noncriminal justice be treated differently than private, noncriminal justice uses?
- Should national security use continue to get a high priority?
- Is there a meaningful distinction between licensing uses and employment uses?
- Should the identity of the prospective user be a criterion for imposing restrictions?



Securing the Integrated Kansas Criminal Justice Information System

By Norma Jean Schaefer and Ron Rohrer[1]
Kansas Bureau of Investigation

Norma Jean Schaefer has worked at the Kansas Bureau of Investigation (KBI) as an Information Technology Consultant since September 1997. Ms. Schaefer assists with network administration, and also provides microcomputer technical assistance and training to KBI staff and microcomputer training to staff from the Attorney General's Office. Ms. Schaefer initiated development of the KBI's intranet Web site

Ms. Schaefer was previously an Information Technology Consultant at the Kansas State Department of Education. She developed, supported and maintained a computerized budget program for all Kansas unified school districts and also provided network administration and microcomputer support. She developed a department intranet Web site and created an intranet oversight committee. As department videoconference coordinator, Ms. Schaefer managed and maintained the videoconference room at the Department of Education and coordinated the statewide videoconference committee.

Ms. Schaefer holds a certification in Novell administration.

I. Background

The Kansas Bureau of Investigation (KBI) was established in 1939 by the Kansas Legislature to combat an increase in the magnitude and complexity of crime in general, and bank robberies in particular. When established, the KBI was directed to conduct investigations at the request of the state Attorney General and local law enforcement agencies, and to maintain state criminal justice records. The KBI later established a crime laboratory, and began assisting in training local law enforcement officers, and providing crime trend information to government officials, local law enforcement agencies, and the public.

The KBI, like many organizations in the criminal justice community, depends on automated information systems to support its operations. A multitude of computer applications are now available that address many aspects of the criminal justice process. The continued, explosive growth in the capabilities of information technology will likely translate into a similar growth in the amount and variety of these criminal justice applications. Kansas has conducted an ongoing effort to manage the growth and integration of its criminal justice information system (CJIS) capabilities, and to provide a cohesive network of automated criminal justice resources. The Kansas Criminal Justice Information System (KCJIS) project is one step toward attaining this goal.

"Internetworking" is a large part of the new technology platform implemented for the KCJIS. Providing access to criminal history information through the Internet and other public networks, rather than implementing a dedicated or private network, provided $1.5 million in annual savings to the state of Kansas, plus more than $1 million in annual savings to local criminal justice agencies, courts and prosecutors.

This paper examines the KBI's method for securing its information network and KCJIS data, reviews the policies that determine the degrees of security installed, and addresses operational and technical issues associated with securing the KCJIS. It is divided into these

[1] Ms. Schaefer is Information Technology Consultant at KBI; her email address is nj@kbi.state.ks.us. Mr. Rohrer is Information Resource Manager at KBI; his email address is Rohrer@kbi.state.ks.us. The authors would like to acknowledge the contributions of Ms. Vicky Harris, Information Resource Specialist, Communications Division, KBI, who serves as Kansas' NLETS representative.

general sections:

- KCJIS architecture and governance structure;
- Components of the new KCJIS, including relevant state and federal policies and/or regulations;
- Security components implemented to secure KCJIS; and
- A look at where Kansas goes from here.

Various consultants and vendors have participated in the development and implementation of KCJIS, and have contributed greatly to the success of the project. They are listed in Attachment A.

II. KCJIS Architecture and Governance

Architecture

Implementation of KCJIS began in 1996 with a budget of slightly more than $10 million. In addition to the KBI, agencies involved in the KCJIS project are: the Kansas Attorney General's Office, the Kansas Highway Patrol (KHP), the Kansas Department of Corrections, the Juvenile Justice Authority, the Division of Information Systems and Communications (DISC), the Federal Bureau of Investigation (FBI), local law enforcement agencies, courts, prosecutors, the state Office of Judicial Authority and the Kansas Department of Revenue.

The KCJIS project, at a minimum, funded the following:

- A new Automated Fingerprint Identification System (AFIS);
- Replacement of a Tandem telecommunications switch with a Microsoft NT Transmission Control Protocol/Internet Protocol (TCP/IP) switch;
- Replacement of a 4.8K-dedicated Systems Network Architecture (SNA) network with a TCP/IP network;
- Re-engineering of the KBI central repository for adult and juvenile criminal history data;
- Local large-system interfaces;
- Free case management system software so local law enforcement agencies can submit electronic Kansas Incident-Based Reporting System (KIBRS) data to the KBI;
- Free case management system software so courts and prosecutors can submit electronic Kansas Disposition Reports (KDR) to the KBI;
- Electronic mail ("email") server and licenses to provide free email accounts to local criminal justice agencies;
- Criminal history World Wide Web server for criminal justice agencies only;
- Criminal history Web server for public data access; and
- A training center and a back-up site.

The system was built following these architectural guidelines:

- KCJIS will be an open system,
- Hardware will be redundant,
- KCJIS will share electronic data,
- KCJIS will use Kansas Wide Area Information Network (KANWIN) and common Internet service providers, and
- KCJIS will spawn appropriate unsolicited email messages.

The software used in KCJIS is Microsoft NT Enterprise, Microsoft Internet Information Server (IIS), Microsoft Exchange, Microsoft SNA, Microsoft Access, C++ and Visual Basic. The hardware used is Dell PowerEdge and Compaq servers. The databases are Microsoft Structured Query Language (SQL) and Microsoft Access.

Governance Structure

A governance structure was developed to effectively plan, manage and operate the KCJIS. The scope of the governance structure is limited to state and local agencies involved in the criminal justice process and noncriminal justice agencies that utilize criminal justice information in licensing individuals. For this paper, we will identify only three of the boards or committees whose approval was required to obtain the security system. More information about the KCJIS governance structure is available on the Internet at http://www.kbi.state.ks.us.

Criminal Justice Coordinating Council

The highest level of authority in the KCJIS governance structure is the Criminal Justice Coordinating Council (CJCC). The CJCC consists of high-level representatives from executive, law enforcement, prosecutiorial, judicial and correctional agencies within the state of Kansas. Members of this group include:

- The Governor
- The Attorney General
- The Director of the KBI
- The Secretary of Corrections
- The Chief Justice of the Kansas Supreme Court or a designee

- The Secretary of Social and Rehabilitation Services
- The Commissioner of Juvenile Justice

The Council provides executive direction and insight to aid state efforts to improve its CJIS. This oversight includes the review, support and approval of improvement initiatives, and the resolution of policy issues as needed. The Attorney General, as chair, and the Governor, as vice chair, provide Council leadership. The Council was formed by the Kansas Legislature in 1994 and will remain in existence until the Legislature deems it no longer necessary.

The responsibilities of the CJCC include:

- Approval and sponsorship of the KCJIS Strategic Plan;
- Approval of funding allocations from federal and state CJIS grant funds;
- Review and response to the activities and recommendations of the KCJIS Advisory Board;
- Approval of any project expenditures; and
- Approval of any changes to the project scope.

KCJIS Advisory Board

The KCJIS Advisory Board is composed of both state and local representatives of key Kansas CJIS stakeholders. State representatives include chief managers involved with CJIS from:

- The Kansas Sentencing Commission
- The KBI
- The Department of Corrections
- The Office of Judicial Administration
- The Kansas Juvenile Justice Authority
- The KHP
- The Secretary of Administration
- The Chief Information Technology Officer
- The Division of Information Services and Communications
- The Department of Education
- The Department of Social and Rehabilitative Services
- The Department of Health and Environment

Local representatives include individuals designated by:

- The Kansas Association of Chiefs of Police
- The Kansas Sheriffs Association
- The Kansas County/District Attorneys Association
- The Kansas District Judges Association
- The Kansas District Court Clerks and Administrators Association
- The Kansas Community Corrections Association
- The Kansas Court Services Officers Advisory Board
- The Kansas Association of Criminal Defense Lawyers
- The Kansas Magistrate Judges Association

The KCJIS Advisory Board advises the CJCC on the progress of existing projects and will initiate discussion of policy or procedural changes required for KCJIS implementation. The Advisory Board is also responsible for briefing the Information Resource Council on new development and implementation of new information technology to facilitate the sharing of information and policies between agencies and branches of state government. Individual members of the Advisory Board act as liaisons with the agencies and associations they represent to ensure that the concerns of those communities are addressed within the KCJIS framework.

Standards and Technology Task Force

The Standards and Technology Task Force is composed of representatives from the following state and local government agencies:

- The KBI
- The Kansas Attorney General’s Office
- The KHP
- The Department of Corrections
- The Division of Information Services and Communications
- The Office of Judicial Administration
- The Chief Information Technology Officer
- The Kansas Juvenile Justice Authority
- Participating counties (Sedgwick, Johnson and Riley are currently participating)
- Participating Cities

One or more of the following skills is required to be a member of the Task Force:

- Database administration
- Telecommunications/networking
- Business systems development
- Operations
- Security

The task force evaluates available information technology to establish standards that enable KCJIS agencies and applications to operate and share information smoothly and effectively, including standards for hardware, software and data across KCJIS project agencies and departments. To date, the task force has established standards for network, hardware, application, data, imaging and messaging. These standards provided for an "open system architecture," which has enabled users to purchase hardware off-the-shelf or by state contract, thereby avoiding the purchase of costly proprietary products and services.

The task force takes direction from the KCJIS Advisory Board to provide a unified direction for KCJIS. Project progress reports and new items of business are presented monthly to the KCJIS Advisory Board.

III. KCJIS Components

The KCJIS components discussed in this section are:

- The Automated Statewide Telecommunications and Records Access (ASTRA) Switch, including national and state security policies that govern it;
- The state repository of criminal history record and juvenile offender information;
- Systems for reporting criminal abstracts, incident-based crime statistics, and criminal case dispositions;
- Private and public Web servers;
- The AFIS; and
- The email server.

ASTRA Switch

KCJIS uses the Automated Statewide Telecommunications and Records Access (ASTRA) system as its current Tandem switch. ASTRA is not Year 2000-compliant and is limited to text-only transmissions. It will be replaced with a redundant NT Enterprise TCP/IP Message Switch, which is capable of sending mugshots and fingerprint images as well as text. The switch software, developed by Paradigm4, is proprietary.

The ASTRA switch is used to access criminal justice information from several national networks: the National Law Enforcement Telecommunications System (NLETS), the National Crime Information System (NCIC), the Kansas Department of Revenue Vehicles Files and the Missouri Department of Revenue Files. The new KCJIS NT switch will be used in the future to access this information as well.

The ASTRA system operates on a 4.8K SNA network that will be replaced with dedicated TCP/IP frame relay and dial-up connections. Dedicated frame relay connections will range in speed from 56K to T1. The state will provide mandated agencies with a 56K frame relay connection to KANWIN.[2] These agencies may opt to increase the connection capacity if they are willing to absorb the price difference. Non-mandated sites may use dial-up or direct connections to the dedicated state frame relay network, or their own Internet Service Provider (ISP).

The state will provide mandated agencies with one personal computer and one copy of Datamaxx software, which is used to query and enter information. All mandated personal computers will use the Windows NT operating system. KCJIS recommends that 911 and dispatch centers use Datamaxx software instead of relying on the performance of a Web browser.

With connections to multiple national systems, many policies and regulations at both the federal and state levels had to be reviewed to prepare Kansas for the transition from a dedicated SNA network to an open TCP/IP network. National policy prohibited the use of TCP/IP networks even though some states were beginning to use them after recognizing the potential of the Internet as a less-expensive means to communicate. The KBI worked very closely with the FBI's Criminal Justice Information Services (CJIS) Division during the transition process. The KCJIS project contracted with Paradigm4 to develop a security document to present to the FBI's CJIS Division that identified a network security strategy that would adhere to current policy while assisting in the creation of new policy. After reviewing staff papers and minutes from meetings of the CJIS Advisory Policy Board and its Security and Access Subcommittee, the KBI discovered that its security strategy was close to their proposed recommendations for disseminating criminal justice information in an Internet environment.

Federal Security Policies Governing ASTRA Switch

The following is a brief

[2] KSA 74-5702 requires the state to establish and upgrade a law enforcement network with a telecommunications connection supplied to each county of Kansas.

description of security policies from NCIC[3] and NLETS with which the current Tandem switch and new TCP/IP Message switch comply.

— *NCIC Security Policy*

NCIC requires that a criminal justice agency be designated in each state as the Control Terminal Agency (CTA). In Kansas, the NCIC CTA is the Kansas Highway Patrol.

NCIC identifies six areas of security in its Security Policy, approved June 1992:

1. **Personnel security**. A thorough background screening, consisting of at least a state and national Interstate Identification Index (III) record check by fingerprint identification and a check against state and national fugitive files, must be conducted for terminal operators, programmers, and any other persons employed or used to conduct any NCIC transactions.
2. **Physical security**. Adequate physical security of the computer and/or terminal must be met to prevent unauthorized personnel from gaining access to the computer and/or terminal or stored data. In addition, documented procedures should be in place to monitor security policies, and operators must use terminals for authorized purposes only.
3. **User authorization**. The FBI assigns Originating Agency Identifiers (ORI) to identify the level of NCIC access each user agency has. This ORI number must be used in each transaction to the NCIC system. In addition, each user accessing NCIC must enter into written agreements with the CTA that outline the access level and NCIC policies that must be adhered to in order to access NCIC data.
4. **Technical security**. Technical security outlines current guidelines for dial-up access and other security recommendations, such as the use of passwords and encryption. It requires that all NCIC “hot file” and III transactions be maintained on an automated log for a specified amount of time. Policy also dictates that this automated log should, in some way, identify the operator on III transactions, as well as the agency for all transactions.
5. **Dissemination**. Criminal justice data stored in NCIC must be protected to ensure correct, legal and timely dissemination and use.
6. **Audit**. Each CTA and/or Federal Service Coordinator is required to audit every terminal agency biennially to ensure compliance with state and NCIC policy and regulations.

The CJIS APB approved the renaming and broadening of the NCIC Security Policy. The new CJIS Security Policy addresses all CJIS systems the APB oversees, including NCIC, NCIC 2000, the CJIS Wide Area Network, the FBI’s Integrated Automated Fingerprint Identification System, etc. Based upon previous CJIS staff papers and minutes of the Security and Access Subcommittee meetings, the state of Kansas was positioned properly when the CJIS APB met and approved implementation guidelines for authentication, dial-up access, encryption and Internet use during its December 16-17, 1998, meeting in Marina Del Rey, California. The following is an outline of those approved policy changes and a description of how Kansas’ network will achieve these requirements.

1. **Authentication**: In addition to the requirement for identifying the agency authorizing a CJIS system transaction, each individual who is authorized to store, process, and/or transmit information on a CJIS system, including those who administer and maintain the systems, shall be uniquely identified. The identifier shall be authenticated. The CTA shall ensure that all NCIC Hot File and III transactions be maintained on an automated log, which identifies the operator on III transactions, the agency authorizing the transaction, the requestor and the secondary recipient.
2. **Dial-up Access**: The CTA has authority to approve and operate dial-in access as long as proper security measures are implemented and managed. The dial-up system shall be able to identify and authenticate dial-in users and the system must be capable of issuing a unique user identity. All CJIS transactions/messages sent and received must be logged. Automatic logging shall include session initiation and termination messages, failed access attempts and all forms of access violations.

[3] Including current NCIC and new NCIC 2000 policies.

The automated log must not be vulnerable to modification if the system is penetrated.

3. **Encryption**: All intelligence information or criminal history record information passing through a public network segment that is not dedicated to criminal justice purposes shall be protected with encryption while in that segment. All CJIS data transmitted over wireless links, dial-up or Internet connections shall be protected with encryption. The use of cryptographic techniques should employ at least 56-bit key, but the segment should apply a more robust key at CTA discretion. Export restrictions also apply.
4. **Internet Access**: Internet access may be granted by the CTA when a minimum set of technical and administrative requirements has been addressed. FBI CJIS criminal history record information — including secondary dissemination through communications media such as Internet electronic mail facilities and remote access file transfer, and any other file modifications — will be permitted through the Internet if the technical security requirements are in place. Hot file inquiries, entries, updates and modifications will also be permitted when the minimum technical requirements for these are in place. Those requirements are:
   - Advanced authentication (such as digital signatures and certificates, biometrics or encryption) to provide assurance that potential users are who they say they are;
   - Access control (using passwords and access control lists, or smart cards and personal identification numbers) to prevent unauthorized access to a service or data; and
   - Integrity (configuration management and anti-virus software, digital signature, encryption) to detect the unauthorized creation, alteration or deletion of data.

— *NLETS Security Policy*

NLETS is a network that was developed to enable law enforcement, criminal justice and other agencies and organizations to exchange sensitive information. This obviously required that policies and regulations be put in place to assure the prevention of network abuses. Like NCIC, NLETS requires that each state designate a criminal justice agency as its Control Terminal Agency. In Kansas, the NLETS CTA is the Kansas Bureau of Investigation.

The NLETS' user community is identical to the NCIC user community. Therefore, it is assumed that if a user conforms to NCIC policy, then adequate controls are in place to assure NLETS network security.

Access to NLETS is controlled by specific hardware and software requirements. NLETS further controls daily access to its network by requiring an authorized ORI, which is also used as an identifier to determine its users' access levels. Like NCIC, the ORI must be a part of every NLETS transmission.

State Policies Governing ASTRA Switch

All state policies and procedures governing the ASTRA switch are approved and adopted by the Kansas ASTRA Board. The following is a brief description of the Board's role and functions, and of the state ASTRA policies.

— *Kansas ASTRA Board*

KSA 74-5701 establishes the Kansas Law Enforcement Telecommunications Committee, called the ASTRA Board. It includes the Secretary of Administration, the director of the KBI, the superintendent of the KHP, a sheriff as designated by the Kansas Sheriffs Association, and a chief of police as designated by the Kansas Chiefs of Police Association.

The board is charged with establishing and upgrading ASTRA, Kansas' law enforcement telecommunications network, an SNA network using dedicated leased lines. The board is tasked with interconnecting each of Kansas' 105 counties with at least one telecommunications connection. The cost of establishing and maintaining this law enforcement network is paid for from funds appropriated or made available by the state Legislature. The cost to purchase and maintain any necessary equipment connected to ASTRA rests with the local county government. The ASTRA Board may also use any available federal funds to maintain the telecommunications network.

Upon approval by the ASTRA Board, additional computers/ terminals may be connected to the telecommunications network. The cost of connection and maintenance of these additional computers/terminals is borne by the agency that installs them.

— ASTRA Policies

Access to ASTRA system information is restricted to criminal justice officials acting in their official capacities. Authority to access ASTRA, NCIC and NLETS is currently limited to agencies assigned an ORI number by the FBI/NCIC. The ASTRA Board may allow other agencies or officials to access ASTRA information when authorized by Kansas Law.

ASTRA requires the same physical security policy on the existing SNA network as does NCIC. ASTRA will maintain this policy in the new TCP/IP network.

ASTRA requires that *all* individuals who operate NCIC terminals be trained, tested and certified in NCIC policy and regulations. ASTRA users fall into two categories: full-access operators and less-than-full-access operators. Full-access operators must, within 6 months of employment or assignment, have a minimum of 4 hours of training, be functionally tested and have their proficiency affirmed by the KHP communications sergeants in order to assure compliance with NCIC policy and regulations. Once operators are trained and tested, they must be functionally re-tested and have their proficiency reaffirmed every 2 years.

The responsibilities of less-than-full-access operators include inquiry capability to one or more NCIC system components. These responsibilities do not include making entries into NCIC. The responsibility for training, functional testing and affirmation of proficiency of these operators, within the first 6 months, is the responsibility of the terminal agency. They, too, will need to be re-tested every 2 years.

All sworn law enforcement personnel must receive basic NCIC training within 12 months of employment or assignment to ensure compliance with NCIC policies and regulations.

All other criminal justice practitioners must have appropriate training for the level of access made available to them by their agencies.

Additional training outlining CTA and Administrative responsibilities is provided, but the Astra Board has not yet mandated it.

Criminal Repository

The KCJIS repository currently resides on an IBM AS400 computing system. It is not Year 2000-compliant and will be replaced with redundant NT servers and Microsoft SQL. Users will access repository information either through the ASTRA switch or through the KCJIS Web server using a Web browser.

The Kansas State Regulation and Policy pertaining to the KCJIS repository is KSA 10-11-1 and KSA 22-4701. The central record repository defined by statute is “criminal history record information” and “juvenile offender information” collected by a criminal justice agency on a person pertaining to a reportable event. This excludes data contained in intelligence or investigation files or police work-product records used solely for police investigation purposes.

According to Kansas’ repository statute, the director of the KBI is responsible for developing procedures to permit and encourage the transfer of criminal history record information among and between courts and the executive branch, and especially between courts and the central repository. The rules and regulations adopted by the director do include the collection, reporting and dissemination of criminal history record information by criminal justice agencies.

Kansas Browser Abstract Reporting System

Today, KCJIS is disseminating criminal abstract information to more than 130 court service officers (CSO) and one major school district via the Web using the Kansas Browser Abstract Reporting System (KBARS). The KBI is using Microsoft IIS and SSL software. Prior to KBARS implementation, it took weeks, if not months, to disseminate criminal abstract information using paper and the mail. KBARS users now access criminal information within minutes. If CSOs or the school district request information on an individual, and that individual’s records are not yet in the KBI’s computerized criminal history (CCH) database, an email message is automatically transmitted to the Records Division instructing it to automate that person’s record. Upon automation of the record, the system sends an email message to the user, urging the user to again access the KBARS to obtain the now-automated information.

Strict rules of dissemination for criminal information and abstracts exist on the repository’s AS400, and these same rules will continue to be applied to information provided through the Web server application for KBARS. The degree of information that will be disseminated is based on the purpose of the information request, and the authority making the request:

- Noncriminal justice employment or licensing,
- Criminal justice employment or licensing,
- Criminal investigation,
- Brady Act firearm purchaser check,
- Pre-sentence investigation, or
- Security guard or patrol employment.

Kansas Incident-Based Reporting

The KCJIS project funded the development of a local law enforcement case management system that, when implemented at the local level, will provide the means to electronically submit data required for KIBRS and NIBRS reporting to the KBI. The case management system is free to all Kansas local law enforcement agencies. KIBRS data will be available at the KBI for ad hoc queries as well as for static statewide reporting.

Kansas Disposition Reporting

The KCJIS project funded the development of court and prosecutor case management systems that, when implemented at the local level, will provide the means to electronically submit to the KBI all the data required for Kansas dispositions. The case management systems are free to courts and prosecutor agencies. The disposition data will be edited prior to the automatic update of criminal history records.

KCJIS Private Web Server

The new KCJIS Web server will reside on redundant NT Enterprise servers using Microsoft IIS software. Users will be able to access KCJIS criminal repository data using any industry Web browser. Local agencies will be able to access this information using the KBARS system. Local law enforcement agencies, courts and prosecutors — with Web browsers and system permission — will be able to access NCIC, NLETS and state Department of Revenue databases. Access through this system is not recommended when response time is critical, such as for 911 and dispatch centers. All other users will recognize significant savings in software and telecommunications costs by using the Web.

Hot files will also reside on the private Web server, and will be updated daily by local law enforcement agencies. The following hot files will be implemented prior to year 2000:

- Be on the Lookout
- Wanted Persons
- Registered Offenders
- Missing Persons
- Probation and Parole
- Involuntary Commitments

KCJIS Public Web Server

The new KCJIS public Web server will reside on redundant NT Enterprise servers using Microsoft IIS software. Data will be replicated from the central repository. Based on current state dissemination rules, only conviction data will be available to the general public. Customers will be able to access public criminal history information for a fee (pre-established account, credit card, etc.) using any industry Web browser.

AFIS

Live-scan units have been or will soon be acquired by 18 local law enforcement agencies in Kansas, in addition to a unit at the Department of Corrections intake facility. Fingerprints and arrest data will be submitted electronically from local live-scan units to KBI on a daily basis. Hit confirmations will be returned on a lights-out basis to local agencies. KBI will submit electronic fingerprint cards to the FBI.

The KBI will use Virtual Private Networking (VPN-1) RemoteLink by Check Point for protection and encryption between the client live-scan site and the host AFIS.

Email Server

The new KCJIS email server will reside on redundant NT Enterprise email servers using Microsoft Exchange software to provide a fast and low-cost means of communicating with the law enforcement community. Many small local law enforcement agencies, courts and prosecutors have not had access to email. This system will provide a way for CJIS agencies to communicate and send information quickly and in a timely fashion. KCJIS users will be able to utilize encryption with email.

IV. KCJIS Security System

Many applications and policies had to be addressed to determine the type and degree of security that KCJIS and the KBI would implement. KBI struggled to provide low security costs to its users while preventing a security risk and administration nightmare. Conversely, adequate security could not be held hostage by the hardware/software and security administration costs. Mr. Ron Rohrer, Information Resource Manager, KBI, played a major role in the security-level decision, stating, "Regarding confidential or sensitive data (especially juvenile data), I will always default to ***security*** versus ***access***. What good is the data if it has been compromised?"

The KCJIS budget provided for preparation of a security report and the purchase of one firewall. While the price for security rose with the purchase of each security component, it was offset by the $2.5 million the state saved each year by using the Internet. Security hardware and software cost KBI approximately $500,000, and certificates and tokens cost KCJIS $175,000. The overall cost savings far outpaced the cost of the security system.

The first step the KBI took in the process of designing its security system was to request a security report from Paradigm4. The company began preparing the report in March 1998 and finished in July 1998. In step two, KBI staff took Paradigm4's report draft and compared it to state and federal policies to identify security system objectives. In step three, Fishnet Consulting, Inc. was selected as KBI's security vendor to recommend software and hardware to meet the bureau's final security objectives, shown in Table 1.

Objective	Vendor Used / Technology Purchased
1. To protect databases stored at the KBI from unauthorized users	Check Point Software Technologies Firewall-1
2. To identify the specific user	Security Dynamics Technologies SecurID tokens
3. To identify the specific device used in a transmission	Entrust Technologies Certificate Authority/PKI
4. To protect data transmissions over a public network carrier	Check Point Software Technologies SecuRemote Encryption
5. To monitor for unauthorized intrusion	Internet Security Systems RealSecure Intrusion Detection
6. To evaluate network security	Internet Security Systems Internet Scanner

Table 1: KBI Security System Objectives

In September 1998, KBI began to obtain the approval necessary to begin installation of the security system. Fishnet Consulting, Inc. installed the system's first firewall the last week of September 1998.

The security products that KBI acquired were in beta test phase or were new releases and all were members of OPSEC.[4] If KBI had started looking at security systems 9 months earlier, it would not have had the integration and security layering needed for an overall secure integrated enterprisewide security system.

While examining the security products it was considering for use, the KBI took into consideration the expertise and experience necessary to implement a large and complicated security system. A significant background in different types of networks, protocols, routers, routing and TCP/IP standards is necessary to establish an effective firewall. No one in Kansas' state government structure had this level of Internet security experience or expertise. Therefore, KBI looked for help in the private sector. The KBI needed someone who could install, implement and maintain its security system for 3 years. KBI also looked for a local expert who could provide around-the-clock, on-site warranty work. Check Point Technologies, Ltd. directed the KBI to Fishnet Consulting, Inc. of Kansas City, Missouri.

Security System Components

Network

Kansas operates its own public network, called the KANWIN. There are two ways to connect to KANWIN: Through a dedicated frame relay connection or through dial-up connections. KANWIN is comprised of state and local government agencies,

[4] Open Platform for Secure Enterprise Connectivity.

K-12 education, universities and hospitals. The KCJIS project will utilize the existing KANWIN frame relay network to reduce telecommunications costs to the state, rather than installing expensive dedicated circuits. The KANWIN network is primarily a TCP/IP network with two T1 Internet connections.

Community of Users

The KCJIS community will consist of a variety of users, from single-device users, to users connected to very simple networks, to complex networks with multiple protocols and network connections. KBI identified these users as:

- Small agencies with no Local Area Network (LAN) will have one or two PC terminals,
- Medium-to-large agencies with a LAN consisting of CJIS and non-CJIS users with multiple PC terminals,
- Metropolitan Area Network (MAN),
- Mobile Data Terminal (MDT), and
- Dial-up users

With these user types in mind, Paradigm4 recommended that two more dedicated frame-relay clouds be constructed from the one KANWIN frame-relay cloud. KBI identified the two new clouds as Open CJIS and Secure CJIS.

— Open CJIS Cloud

This network is comprised of KCJIS and non-KCJIS users connected to the same LAN. Their networks can be small to very large with connections to other LANs via MANs. This network was designed for availability, not security. It separates KCJIS traffic from all the other KANWIN users. These users are required to have adequate protection between their LANs and their connections to the Open CJIS cloud. KBI recommends that these agencies install access control devices between their LAN and any other agency LAN connections.

— Secure CJIS Cloud

This network is for KCJIS users only who will have dedicated frame-relay connections to the cloud. Users *cannot* have non-KCJIS users on or connected to their LANs. Users residing on this cloud are mainly small LANs made up of up to 20 PCs. This network cannot have any modem permanently attached to any PC or network. The secure CJIS cloud has its own core backbone routers dedicated solely to secure KCJIS. The cloud is protected by redundant firewalls. All secure CJIS traffic must transverse through these DISC[5] firewalls.

Network Security Policies and Procedures

Not all necessary or required security policies and procedures have been determined, approved and implemented at this time. Current network security policies (as of August 1998) were put together by a subcommittee appointed by the ASTRA Board, and approved and adopted by the Board in September 1998. These can be viewed on-line at: http://www.kbi.state.ks.us. Changes have been made since then affecting the security policies in place, which the ASTRA Board is expected to review at its January 1999 meeting. The security policies are working documents that change as security needs change, and are included in this report as attachments B through D, as follows:

- Network policies are included as Attachment B,
- Computer and network use policies are included as Attachment C,
- Email acceptance use and Internet policies are included as Attachment D. (All KBI staff members are required to attend email and Internet use training and sign the policy, which is kept in their personnel files.)

Current ASTRA network security policies state that KCJIS users may dial up local ISPs or the KANWIN to access KCJIS.

Security Objectives/Products

Protecting Databases from Unauthorized Use: Firewalls

To meet our first objective — protecting databases stored at the KBI from unauthorized users — KBI purchased redundant Check Point FireWall-1, which included Check Point's firewall, management, inspection and triple data encryption standard (DES) modules. KBI chose Check Point's FireWall-1 because of its Stateful Inspection, open architecture and VPN capabilities, as well as for its capability to manage multiple firewalls from a centralized location. An important decision factor was Check Point's work with OPSEC. This increased KBI's options to purchase third-party products to enhance security levels through

[5] Division of Information Systems and Communications.

layering.

Because the firewall is the only way in and out of KCJIS, KBI needed the firewalls to be in a "hot standby" configuration. Fishnet Consulting recommended StoneBeat software for this purpose. StoneBeat is high-availability software that will protect the system against single-point hardware failure and that will allow KBI to perform firewall software and hardware maintenance without interrupting its operation. The two firewalls are connected by Ethernet out-of-band connections.

The primary and secondary firewalls are identical with respect to hardware configuration and FireWall-1 software. A switch-over procedure is activated if the primary firewall fails. If failure occurs, the secondary firewall will reconfigure its network interfaces by using the exact same IP and MAC addresses as the primary firewall. Therefore, the switchover is completely transparent to other IP devices. All connections are preserved during the switch over; the user will see only a short delay.

Both firewalls have Chrysalis encryption network interface cards (NIC). These cards offload encryption from the central processing unit (CPU) of the firewall to the NIC card. Every packet coming to KCJIS is encrypted; therefore, a system was needed to offload encryption from the CPU for performance.

Chrysalis cards are capable of T1 to Fast Ethernet speed connections and can integrate with the Check Point Firewall-1 VPN solution. The cards will accelerate the cryptographic functions of standard IPSec using ISAKMP[6]/Oakley key management. The cards use memory on the card and processors to perform authentication, key generation and encryption.

Identifying a Specific User: Secure ID Tokens

To meet our second objective — identifying the specific user — KCJIS purchased Security Dynamics Ace Server and key fob tokens. There was, and still is, a lot of discussion about the decision to use Security Dynamic's key fob tokens in place of static passwords to access KCJIS.

SecurID tokens combine "something you know" with "something you have" to identify each user accessing KCJIS. This is known as strong authentication. There were many advantages, and only one disadvantage to using them. The advantages far outweigh the disadvantage, which was cost, since the tokens were not included in the budget.

One of the most important advantages was security. Each password is used only one time, making the system extremely secure even if a password is stolen. Another advantage was user authentication management. The policies approved by the ASTRA Board in September 1998 stated that all passwords for KCJIS users must be six characters in length and consist of both letters and numbers. Passwords will also change every 30 days. A policy this stringent was necessary because most users choose passwords poorly. However, this approach often encourages users to write their passwords down and, more than likely, leave them close to their PCs. Passwords are not always effective, as "hackers" have tools such as "Cracker" and "Social Engineering" available to steal them. KCJIS predicts that its user base will grow to 12,000. Managing that many passwords is an enormous task for any help desk. SecurID tokens provide a very secure method for accessing KCJIS, and they make it easier to manage user passwords.

As for the disadvantage of using SecurID tokens, security costs were not included in the initial KCJIS design. Users were not informed of the cost until September 1998, the same month that installation of security and implementation of the ASTRA switch took place. KCJIS purchased 4,000 tokens with the intent to distribute 10 tokens to each agency that accesses ASTRA. These tokens last for 18 months. This was done to eliminate some of the financial burden on agencies unable to purchase tokens for users. For most agencies, deployment of the tokens fell at the end of one budget year, and the beginning of the next. Purchasing 18-month tokens allowed agencies to budget for renewal tokens in May 2000. All agencies with additional users will be required to purchase the additional tokens. Agencies may purchase them directly from a reseller or by using a state contract.

KCJIS users will use tokens to log on to each system. Unlike Single Sign-On, which allows users to sign-on to the system only once and to gain access to all resources for which they are authorized, SecurID requires each user to sign on to each resource separately. This provides KBI

[6] Internet Security Association and Key Management Protocol.

with a log of every access attempt to each device.

All KCJIS users fill out applications providing KCJIS with information about each user. Along with title and mailing information, KCJIS users select a secret word they use to identify themselves over the telephone, if necessary, to replace a lost token or reset a token. Tokens can be transferred from a departing employee and reassigned to a new employee. Policies and procedures are currently being drafted.

Identifying Specific Transmission Devices: Certificates

To meet the third objective — identifying the specific device used in a transmission — KCJIS became its own Certificate Authority (CA). (A CA is a trusted entity that vouches for the identity of an individual using a system.)

KCJIS is using Entrust Technologies' PKI solution, its X.509 Digital Certificates. All personal computers accessing KCJIS will be required to have a certificate issued by KCJIS. KCJIS purchased 2,500 certificates to be distributed to users with existing ASTRA access. KCJIS purchased these certificates to eliminate a financial burden on agencies. Deployment of certificates caught the users between the end of one budget year and the beginning of another. These certificates do not expire until 2001. This will allow users plenty of time to budget for renewed certificates.

KCJIS chose to certify only the PC terminals, as SecurID tokens were being used to identify users. KCJIS needed to identify PC terminals so when KBI audits a location, it could verify the particular PC terminal used. In most locations, employees working different shifts use one terminal. If each user was certified individually, he or she could only log on to the PC where his or her certificate resided. Also, if that PC broke down, the user could no longer log on to KCJIS until it was fixed or until a new certificate was issued for a different PC.

The certificates purchased are for digital signing and encryption, and provide data integrity through hashing to verify that transmitted data were not changed in transit. The certificates also provide nonrepudiation, or proof of origin. KCJIS enjoys these benefits by being its own CA:

1) KCJIS controls ownership and use of the CA's private signing key;
2) KCJIS controls who obtains certificates, and
3) KCJIS controls sensitive information specific to the KCJIS user community.

Because Entrust is integrated into Check Point's SecuRemote software, the user configures some settings under the Entrust menu in SecuRemote and obtains their signing and encryption keys electronically.

Protecting Data Transmissions: Encryption

To meet the fourth objective — protecting data transmissions over a public network carrier — KCJIS is using SecuRemote software with triple DES encryption (168 bit) by Check Point, to create a VPN between the user and the KBI firewalls.

SecuRemote will be used for all connections to KCJIS. The software runs on Windows 95 and Windows NT desktops and laptops. SecuRemote supports all IP-based network communications. This software was *free*.

SecuRemote maintains information about the KCJIS site or encryption domain. Each time a user requests a connection, SecuRemote intercepts the request and determines whether the destination resides within the KCJIS encryption domain. Once the KCJIS FireWall-1 has been identified, SecuRemote automatically invokes a challenge to the user for proper authentication.

After the user is successfully authenticated to the KCJIS-supplied certificate, SecuRemote validates the Entrust certificate on a user's behalf to initiate an Internet Key Exchange (IKE) key negotiation with the KCJIS FireWall-1 and establishes a secure VPN tunnel. All VPN functionality, including key negotiation and data encryption, is completely transparent to the user. Session keys are updated throughout the duration of the connection at a specified amount of time.

KCJIS purchased Netscape's Lightweight Directory Access Protocol (LDAP) Directory Server. This allows KCJIS to store all user data in a LDAP directory. The LDAP directory has many benefits, such as separating the user/group data store from the server to achieve scalability. This way, a single LDAP server can search and manage millions of user entries at a time. Second, it can be used not only to store user and group data, but also to access control lists, X.509v3 certificates, client preferences and server configurations. LDAP directories have modifiable schemas that allow storage of any type of application information.

KCJIS maintains information on each user, including the user's full name, login name, email address, authentication scheme, authentication server, authorized sources, authorized destinations, time restrictions, encryption key negotiation scheme, encryption algorithm, data integrity method and group membership.

Once the LDAP directory server is populated with KCJIS user information, new LDAP-capable servers installed into the same environment can share that data by accessing the same installed directory. Access to shared directory information is accomplished through the Internet Engineering Task Force (IETF) standard LDAP protocol.

One of the biggest benefits of the LDAP Directory Server is manageability. KCJIS data can be accessed through a shared centralized administration console. If a user's access must be revoked, KCJIS administrators will be able to revoke the user in all security servers from one main console. If KCJIS did not deploy an LDAP directory server, the user would have to be revoked separately from each individual security server. This is a huge administration burden for the KBI help desk, which must serve a community of 12,000 users.

LDAP plays an important role in user authentication. The KCJIS firewall attempts to authenticate a user against information stored in the user's entry in the LDAP directory server. The user either passes or fails. If the user fails, then the session is closed. If successful, the key exchange then takes place and a VPN is created.

Because of the need for utmost security of the LDAP directory and of the information it contains, no one will be able to query information from anywhere other than the console or the KBI help desk. KBI recommends that some information be duplicated to an additional LDAP directory server that will reside at DISC's facilities on a DMZ. This will provide a directory server for KCJIS users to query email and public key information regarding KCJIS users.

Monitoring Unauthorized Intrusion: Intrusion Detection

To meet the fifth objective — monitoring for unauthorized intrusion — KCJIS purchased RealSecure by Internet Security Systems.

Protecting the KBI LAN from intruders and unauthorized activity internally and externally is one of the most critical responsibilities of security management. RealSecure is a real-time attack recognition and response system. RealSecure provides the highest level of protection against attacks. It will enable KBI to dynamically detect suspicious network activity and instantly prevent unauthorized access.

RealSecure analyzes information packets as they travel across the network. It recognizes traffic patterns that indicate hostile activity or misuse of network resources, including network attacks. RealSecure can immediately alert KBI network administrators of any suspicious activity, log the session and automatically terminate the connection.

RealSecure can respond to unauthorized or suspicious activity automatically by logging, recording or terminating actions, and can dynamically reconfigure firewalls.

Evaluating Network Security: Internet Scanner

To meet the sixth objective — evaluating network security — KCJIS purchased Internet Security Systems' Internet Scanner v. 5.6 to continuously access the KBI firewalls and LAN devices to identify vulnerabilities in configurations. Internet Scanner identifies security weaknesses in Windows NT and network configurations. Internet Scanner utilizes a comprehensive and dynamic database of attacker methods and vulnerability tests.

KBI will be assessing firewalls and KBI LAN continuously. The slightest misconfiguration to a firewall or a server due to human error leaves the system vulnerable to attack. KBI has also contracted with Fishnet Consulting to conduct security analysis. DISC has acquired different products to provide KBI with other assessment tools.

KCJIS Backup Site Disaster Recovery

KCJIS has provided for a cold site to be built at the Kansas Highway Patrol in Salina. This site will house the backup ASTRA switch along with the same security system installed at the KBI with the exception of RealSecure and Internet Scanner. This site would only be used if a disaster occurs rendering the KBI's main site inoperable.

Not only does the cold site provide for backup in case of a disaster, it also provides a duplicate system to test patches and upgrades. Fishnet Consulting will perform maintenance on these systems before performing them on the live security servers. All databases will be restored from backup tapes to this site during maintenance. Backups of all security servers are performed routinely and taken offsite.

IV. Where do We go From Here?

The KBI realizes that its network is a stepping stone to national networks. Therefore, there are several security areas that KBI will continue to assess and enhance. Listed below are just a few of the areas we identified.

Securing Servers and Computers

The KBI is in the process of securing all devices on the KBI internal LAN, thus providing another layer of protection. This will safeguard data if an unauthorized individual gains access to the network, as well as provide protection from internal users intent on mischief. The KBI will use Internet Scanner to identify security weaknesses.

Security Staffing

Security is a full-time job. The KBI is assembling teams to work toward the continuously improved security. Teams will be assigned with specific duties, ranging from legal to technical responsibilities. The KBI has identified two qualified KBI staff members whose work assignments are being converted from technical to security positions. In addition, the KBI's fiscal year 2000 budget requests funding security full-time equivalents (FTEs).

Emergency Response Planning

The KBI maintains an in-house "Computer Crime Division" that will direct planning and drills to prepare for attacks on KCJIS, which could realistically occur despite the amount of security precautions that have been taken. This realization keeps KBI consistently monitoring, analyzing and fixing vulnerabilities, moving toward continuous security improvement.

Compliance Auditing

Every user and every device is identified to the system. Monthly message switch activity reports (plus ad hoc reports) assist KBI compliance auditors in quickly spotting exceptions that might require on-site visits to local ASTRA users. Our objective is to automate compliance audits as much as possible, and to reduce the amount of travel time required to maintain proper compliance.

Training

By March 1999, Paradigm4 is planning to deliver a Training Information System database that identifies all users and records their level of NCIC access training. The system will automatically generate emails to both users and their supervisors, when users approach the time for NCIC retraining or recertification. The first email message will be sent approximately 90 days prior to expiration. If a particular user's training or certification has expired, the software will *not* allow the user to access the KCJIS databases.

Security training will also be supplied to KCJIS users and KBI staff. Users need to be trained on security components and how to use the components securely to protect access to the KCJIS systems as well as to their own computer.

V. Conclusion

A good security plan addresses both security objectives and policies. The KCJIS does not have a formal "security system," rather an ongoing security plan and direction. Its "security system" is simply where it is at any given moment.

Attachment A: KJIS Security Products and Vendors

Security Products Used in KJIS

Check Point Software Technologies, Ltd.
3 Lagoon Dr., Suite 400
Redwood City, CA 94065
Phone: (650) 628-2000
Fax: (650) 654-4233
Contact: info@checkpoint.com
http://www.checkpoint.com

Chrysalis-ITS
1688 Woodward Dr.
Ottawa, Ontario, Canada K2C 3R7
Phone: (613) 723-5077
Fax: (613) 723-5078
http://www.chrysalis-its.com

Compaq Computer Corp.
P.O. Box 692000
Houston, Texas 77269-2000
Phone: (281) 370-0670
Fax: (281) 514-1740
http://www.compaq.com

Dell Computer Corp.
1 Dell Way
Round Rock, Texas 78682
http://www.dell.com

Entrust Technologies
2323 N. Central Expressway
Suite 360
Richardson, Texas 75080
Phone: (888) 690-2424
Fax: (972) 994-8005
E-mail: entrust@entrust.com
http://www.entrust.com

Internet Security Systems, Inc.
Headquarters
6600 Peachtree-Dunwoody Rd., Bldg 300
Atlanta, GA 30328
Phone: (678) 443-6000
Fax: (678) 443-6477
http://www.iss.net

Microsoft
1 Microsoft Way
Redmond, WA 98052-6399
Phone: (425) 882-8080
http://www.microsoft.com

Netscape Communications Corp.
501 E. Middlefield Rd.
Mountain View, CA 94043
Phone: (650) 254-1900
Fax: (650) 528-4124
http://www.netscape.com

Printrak International, Inc.
1250 N. Tustin Ave.
Anaheim, California 92807
Phone: (513) 683-8210
Fax: (513) 683-0903
http://www.printrakinternational.com

Security Dynamics Technologies, Inc.
20 Crosby Dr.
Bedford, MA 01730
Phone: (781) 687-7000
http://www.securitydynamics.com

Stonesoft, Inc.
115 Perimeter Center Pl.
South Terraces, Suite 140
Atlanta, Georgia 30346
Phone: (770) 668-1125
Fax: (770) 668-1131
http://www.stonebeat.com

KCJIS Vendors

Business Software and Equipment, Inc.
8655 College Blvd.
Overland Park, Kansas 66210
Phone: (913) 327-1133
Fax: (913) 451-8716
E-mail: itafanelli@bsekc.com

Datamaxx Applied Technologies, Inc.
3780-A Peddie Dr.
Tallahassee, Florida 32303-1148
Phone: (850) 575-1023
Fax: (850) 575-0689
Email: ccowens@datamaxx.com

Division of Information Systems and Communication (DISC)
900 SW Jackson
Landon State Office Building
Topeka, Kansas 66612-1251
Phone: 785-296-3463
http://www.ink.org

FishNet Consulting, Inc.
601 Walnut, Suite 202
Kansas City, MO 64106
Phone: (816) 421-6611
Fax: (816) 421-6677
E-mail: info@kcfishnet.com

MTG Management Consultants, L.L.C.
1111 Third Ave., Suite 2700
Seattle, Washington 98101-3201
Phone: (206) 442-5010
Fax: (206) 442-5011
E-mail: mtg@mtgmc.com

Paradigm4
885 Third Ave., Suite 450
New York, New York 10022
Phone: (212) 303-5591
Fax: (212) 303-5555
Email: jbay@paradigm4.com

Attachment B:
KJIS Policies

KCJIS Network Security Policies

1. Agencies shall assure that access to or modification of CJIS sensitive data is made only by authorized users.
   - A. All CJIS sensitive data shall be encrypted when passing through a public carrier network or any private network not dedicated to Criminal Justice use.
   - B. Each user accessing the system shall have a unique user ID.
   - C. Each user ID shall have an associated password. Valid passwords shall be at least 6 characters in length and shall consist of both letters and digits. Passwords shall be valid for 30 days.
   - D. All dial access into the secured CJIS network shall be via the DISC provided dial services. Dial modems are not allowed inside the secured network except as outlined in Technical Policies paragraph 2.E.
   - E. Specific security standards shall be put in place by each agency regarding the access to the State CJIS system. These standards shall include: Internet Policies, Remote Site Policies, and Mobile Data Terminals (MDT) policies.
   - F. The following types of Dial-in accesses are permitted from the Open CJIS network. Dial access must comply with one of the following. This access must comply with the current version of the Paradigm4 CJIS security report, Phase II, paragraph 4.1.1.
     1. Locally provide (Modem Pool).
     2. Users access through an Internet Service Provider (ISP) as long as it complies with other security policies.
   - G. Access to the secured CJIS network from the open CJIS network shall occur only through the DISC network firewall.
   - H. Agency LANs shall provide adequate protection to the CJIS devices on the LAN. This protection may include firewalls or similar access devices as well as server/PC-level access control (logon “id”, etc.). It is the responsibility of the agency head to ensure that only CJIS authorized users are able to view CJIS data or issue CJIS transactions.
   - I. All requests for connection to the open or secure CJIS network shall include a description of how the site meets the network & technical security policies as defined or the level of connection requested.

Personnel Security Policies

An agency with access to CJIS information shall assume responsibility for and enforce CJIS System security policies. Specific personnel security standards shall be met in instances where agencies access the CJIS Network, NCIC and/or III information. Personnel included by the policy include: Full time, part time, temporary and contract employees that have access to CJIS systems. These standards include:

1. No one can have access to the CJIS systems that has been convicted of a felony or severe misdemeanor.
2. A background check, minimally including; (1) local name check, (2) State and Federal name and fingerprint check, (3) local and Federal warrants check, shall be conducted.
3. All personnel that have access to the CJIS system shall be at least 18 years old.
4. Each agency authorized to receive CJIS information shall have an appropriate written standard for discipline of CJIS policy violators.
5. Agencies shall have procedures in place regarding changing of passwords, etc. of terminated employees.

Physical Security Policies

1. The criminal justice agency shall ensure the computer site and any related CJIS equipment shall have adequate security to protect against unauthorized person(s) from gaining access to the computer, network and/or data.
2. Agencies shall have policies in place regarding physical security of MDT's and remote access users.

Technical Policies

Policies in this section encompass general technical issues involving networks and authentication including management and support of the secured CJIS network and LANs connected to the secured network.

1. Network Management, Diagnostics, and Repair
   - A. DISC shall be responsible to ensure the 7x24 availability of the secured and open CJIS networks, in accordance with the service level agreements(s) implemented between DISC and the Kansas Criminal Justice Coordinating Council.
   - B. Third party vendors, consultants, etc., employed to perform maintenance or network service shall be monitored. It shall be the responsibility of the criminal justice agency to ensure no CJIS sensitive data is allowed to leave the site without prior approval. A log of CJIS sensitive data which has left the site shall be maintained for two years.
2. Access to Secured CJIS network.
   - A. Shall be a criminal justice agency with no other non-criminal justice agency on their LAN and/or WAN.
   - B. A LAN connected to the secured CJIS network shall have only one access point to or from the LAN; that being the router connection to the secured CJIS network.
   - C. Traffic to or from an agency on the secured CJIS network shall be for Criminal Justice or law enforcement business purposes only. It is the responsibility of the agency to ensure compliance with this policy.
   - D. Any dial access shall be authenticated and logged at the time of connection. All backups, or other copies of CJIS information taken from the CJIS servers shall be protected to ensure no unauthorized access to the data is possible if removed from the secured physical location.
   - E. No modems shall be permanently connected to the LAN on the secured CJIS network. Controlled modem access is permitted when the modem is enabled only during the time the dial in was necessary and immediately disabled.
   - F. DISC may employ additional monitoring as necessary to isolate network problems on the secured and open CJIS networks. With the owning agency's approval, DISC may employ additional monitoring as necessary to isolate network problems that appear to be originating from a local LAN.

No local firewall(s) will be required at agencies connected to the secured CJIS KANWIN.

Training Policies

1. All CJIS terminal users that operate CJIS terminals should be trained to their level of access within six months of employment. The following outlines the training that each level of personnel shall achieve:
   - A. All full-access operators shall pass the NCIC certification test given by the Kansas Highway Patrol. This certification shall be renewed every two years. If certification expires, the operator will not be allowed on the network until re-certification is completed.
   - B. All less-than-full-access operators shall be tested by the employing agency, and re-tested every two years to ensure operators proficiency. The employing agency shall keep documentation of all training that it provided and documentation shall be provided during audits. In addition, the Kansas Highway Patrol shall be notified of the names of all less-than-full-access operators, and the dates of their certification.

C. All sworn law enforcement personnel shall receive basic training in NCIC matters adhering to the minimum curriculum recommended by NCIC in order to ensure effective use of the system and compliance with the NCIC policies and regulations. The employing agency shall keep documentation of all training that it provided and documentation shall be provided during audits.

D. The agency shall provide training to the level of access permitted for criminal justice practitioners. This would include such personnel as record clerks, court clerks, district attorney's etc. The employing agency shall keep documentation of all training that it provided and documentation shall be provided during audits.

E. Within six months of election, selection or assignment, criminal justice administrators and upper level supervisory personnel shall obtain training concerning capabilities of the CJIS Network, regulations, policy, audit requirements, sanctions and related civil liability problems. This training is designed to familiarize administrators with the key issues that affect their agency. The employing agency shall keep documentation of all training that it provided and documentation shall be provided during audits.

F. All personnel assigned to technical and supervisory positions with access to the CJIS system shall have received approved training within 6 months of their appointment.

2. All personnel with CJIS access shall be trained on privacy and security issues regarding criminal history record information. Once trained, all personnel shall sign awareness statements showing that they understand the penalties and/or circumstances of misusing Criminal History Record Information (CHRI).
3. All CJIS terminal users should be provided network security awareness training within 6 months of employment.

Administrative Security Policies

1. Record Keeping
   Each agency is held responsible for their record keeping practices. This information will be monitored through compliance audits.
2. Destruction/Disposal
   All information received from the CJIS Network shall be destroyed when no longer needed.
3. Documentation
   Documentation that supports any operations on the CJIS Network, training personnel, security violations, etc., shall be provided to authorized audit staff upon request.
4. Notification
   If a violation of security is discovered the discovering agency shall notify the state NCIC Control Terminal Officer (CTO) without delay. Immediate reporting of such violations is expected. In any event, the discovering agency shall ensure that the state NCIC CTO is notified of such violation within one business day.
5. Administration
   Each agency shall appoint a Terminal Agency Contact (TAC) who shall serve as a focal point for the CJIS issues, including these Administration policies.

Audit Policy

The Kansas Criminal Justice Coordinating Council (KCJCC), Federal Bureau of Investigation (FBI), Criminal Justice Information system (CJIS) Advisory Board, and Kansas Law Enforcement Telecommunications Committee (ASTRA) have charged the Kansas Bureau of Investigation (KBI) and the Kansas Highway Patrol (KHP) with the audit responsibilities for the CJIS Network.

Those responsibilities are created through the following statutes, rules and regulations and/or policies.

1. FBI Security Policy 2.K.S.A. 22-4704 3.K.S.A. 74-5701 4.K.S.A. 74-5702
   Periodically, the KBI and/or the KHP will conduct audits to assure compliance with established policies. During the on-site audits at least the following areas may be reviewed.

1. Network Security
2. Personnel Security
3. Physical Security
4. Technical Security
5. Training Issues
6. Administrative Security

Additional areas will may also become part of the periodic audits that are not included in the policies listed above. Those areas are listed below.
1. Information Quality
2. Dissemination
3. Validation Review
4. NCIC Quality Assurance
5. Kansas Hot Files Quality Assurance

Each agency shall respond to the NCIC CTO or his designee, in writing within 30 days of receiving any final audit report, where an area is non-compliant.

If areas of non-compliance are not corrected the report will be referred to the NCIC CTO will determine the appropriate sanctions, or termination of service.

As a result of the auditor's findings and recommendations outlined in the final audit report, sanctions may be recommended to the NCIC Control Terminal Officer. The CTO will notify the local agency of any sanctions or other required changes.

Attachment C:
KBI Computer and Network Policies

Computer and Network Usage Guidelines DRAFT

1.0 Computer Usage Policies

- All employees, vendors, and contractors are required to sign a KBI Security Policy before accessing any KBI computer system.
- Employees must have an authorized user account assigned to them prior to accessing any KBI computer system.
- Employees may access only those resources for which they are specifically authorized.
- Employees are personally responsible for safeguarding their account and log-on information. Passwords must adhere to the following:
    - Passwords must remain confidential
    - Passwords must be changed every 60 days.
    - Passwords must be at least eight (8) characters in length and should use a combination of alpha, numeric and special characters.
    - Passwords must not identify the user, either through name, date of birth, family member names, etc.
    - Passwords must not be common words
    - Passwords must never be displayed, printed, or otherwise recorded in an unsecured manner.
- Employees are not permitted to script their user Ids and passwords for log-on access.
- Employees are not permitted to allow another person to log-on to any computer utilizing their account information, nor are they permitted to utilize someone else's account information to log-on to a computer.
- Employees may not leave their workstation logged onto the network while away from their desks.
- Employees may not load any software onto any KBI computer without the direct permission of the Information Resource Manager.
- Employees should promptly report log-on problems on any other computer errors to the Data Processing Team. Errors sometimes indicate previous unauthorized access attempts.
- Employees should promptly notify the Information Resource Manager if they have any reason to suspect a breach of security or potential breach of security.
- Employees should promptly report anything that they deem to be a security loophole or weakness in the computer network to the Information Resource Manager.
- Employees may not install or use any type of encryption device or software that has not been approved by the Information Resource Manager, for use on their computer system.
- Employees may not disable any authorized encryption device or software program.
- Employees may not disable any virus program.
- Employees may not copy any software from any KBI computer system for personal use. If an employee requires additional copies for new users, they are required to purchase additional software licenses for KBI use.

- All removable media (i.e. floppy diskettes, tapes, CDs, etc.) must be clearly labeled as to the content of the media and should contain, at a minimum, the date, and owners name.
- Employees may not utilize KBI computer systems for any of the following reasons:
  - Unauthorized and time consuming game playing;
  - Non-related work activity; or
  - Any illegal activity.
- Employees are prohibited from intercepting or monitoring network traffic by any means, including the use of network sniffers, unless authorized by the Information Resource Manager.
- Use of any part of the KBI's computer network will acknowledge acceptance of all rules, regulations, policies, and procedures in effect at that time.
- Employees may not give out any computer information over the telephone to anyone, regardless of who they claim to be. Individuals involved in "social engineering" are usually able to get valuable corporate information from employees through trickery.
- All data storage media must be erased or destroyed prior to being placed in the trash.

2.0 Virus Protection

Each computer system must execute a virus protection program at boot-up, which has been approved by the Information Resource Manager. If an employee does not have one, he/she is directed to notify Data Processing as soon as possible.

- No employee shall copy, distribute, or introduce any software known or suspected of being infected with a virus onto a computer system.
- If an employee's computer or diskette has been found to contain a virus, the employee must notify Data Processing immediately. The employee should supply Data Processing with information which includes names of type of virus, software used to detect the virus, extent of infection, source of virus, potential recipients of infected material, and steps taken to disinfect the virus if any.
- Any file or diskette received from an outside source must be scanned by the approved virus scanning program, before being introduced onto any computer system.
- No shareware games, utilities, or any other shareware file may be loaded onto any KBI computer system.

Attachment D:
KBI Internet and Email Policies

Acceptable use of the Internet Effective Date: January 16, 1998

1.0 PURPOSE: To establish an Internet Use policy for KBI employees.

2.0 DEFINITIONS:

Official State Internet Use is the access to or distribution of information via the Internet by state officers or employees which is in direct support of Official State Business. “Official State Business” is defined in K.A.R. 1-17-1 as “The pursuit of a goal, obligation, function, or duty imposed upon or performed by a state officer or employee required by employment with this state.”

Other Appropriate Use. By authorizing the payments for access to KANWIN and/or the Internet Service Provider the KBI Director has the implicit authority and responsibility to determine when and under what circumstances the officers and employees of the KBI can use the Internet for activity other than described above. (KIRC Policy #1200 Revision #0, 6.0, 6.1, 6.2)

3.0 POLICY:

Privilege of Internet access is provided to employees to conduct “Official State Business.” Officers and employees of the KBI can use the Internet for other than official business, unless the KBI Director has deemed certain individuals as not having this privilege. Officers and employees of the KBI will not cause the KBI to incur any costs associated with the use of the Internet for other than official business.

Any officer or employee of the KBI who violates the provisions of the KBI’s policies and/or procedures regarding Internet activity, shall be subject to disciplinary action, including, but not limited to, demotion, suspension, and termination. In every case, however, the offending officer or employee shall be required to reimburse the state for the total value of any damage to state property and Internet fees incurred in violation of this policy and of any state established policies and procedures.

4.0 PROCEDURES:

ACCESS TO INTERNET: Access to the Internet is provided if connected to the KBI headquarters Local Area Network (LAN). In the field offices, obtaining Internet service from an Internet Service Provider (preferably KANWIN) must be approved through the Division Head.

Administrative Implemented Procedures

- There will be NO files downloaded from the Internet unless authorized by the Information Resource Manager, Data Processing.
- There will be NO installation of software downloaded from the Internet unless authorized by the Information Resource Manager.
- Should any viruses be found, Data Processing should be notified immediately.

MODEMS:

Headquarters

- There will be NO modem installed to any PC that is connected **directly** to the KBI Headquarter LAN. Employees needing modem access to the Internet for KBI duties will be provided an alternative by Data Processing.

Field Offices

- Upon completion of installation of LAN, there will be NO modem installed to any PC that is connected directly to the KANWIN.

EMAIL:

KBI encourages employees to learn to use electronic mail and telecommunications tools and apply them in appropriate ways to the performance of tasks associated with their positions and assignments.

Administrative Implemented Procedures

- KBI employees shall communicate with telecommunication tools in a professional manner consistent with state laws and KBI policies governing the behavior of KBI employees and with federal laws governing copyright.
- All KBI employees can acquire an Email account, if approved by their Department Heads.
- Officers and employees in the field will be responsible for obtaining approval from their Department Head to acquire access to the Internet.
- All KBI employees WILL use secure authentication AND encryption to exchange sensitive Email. Authentication can be acquired only from the KBI Information Resource Manager.
- Any file received as an attachment in an email message MUST be scanned for viruses before opening.

EMPLOYEE DISCLAIMER NEWSGROUPS/ MAILING LISTS/ EMAIL:

All KBI officer’s or employee’s view points posted in one of these methods must be in accord with official policy.

5.0 PRIVACY:

Employee electronic records are public records and employee work products, therefore, files and messages may be accessed or activities monitored under the following circumstances:

- Routine system maintenance;
- General inspection or monitoring, with or without notice;
- Specific review of individual files or monitoring of individual activity, with or without notice; and
- In the event of a public records request. An exception to disclosure are investigative files and communication relating to investigations.

6.0 UNACCEPTABLE USE: The following uses of KBI’s Internet access/Email are NOT permitted on the part of KBI employees:

- Personal use of the Internet/Email during your regularly scheduled work hours. (Lunch hour at your Department Head’s discretion.)
- Breaks;
- Transmitting obscene, abusive, sexually explicit, or threatening language;
- Violating any local, state, or federal statute;
- Using other employees passwords;
- Vandalizing, which is any unauthorized access and/or malicious attempt to damage computer hardware/software or networks or destroying the data of another user, including creating, uploading, or intentionally introducing viruses;
- Intentionally wasting limited resources;
- Using the network for commercial purposes;
- Harassing, insulting, or attacking others;
- Gaining unauthorized access to resources or entities;
- Political and lobbying activities;
- Collective bargaining activities;
- Fundraising activities, unless they are government approved or sponsored;
- Seeking to gain or gaining unauthorized access to information resources or other computing devices unless part of KBI duties; and
- Breaking copyright laws.

7.0 MONITORING: **All Internet use by employees can and will be monitored.**

8.0 CANCELLATION: None

Bureau of Justice Assistance Information

General Information

Callers may contact the U.S. Department of Justice Response Center for general information or specific needs, such as assistance in submitting grants applications and information on training. To contact the Response Center, call 1–800–421–6770 or write to 1100 Vermont Avenue NW., Washington, DC 20005.

Indepth Information

For more indepth information about BJA, its programs, and its funding opportunities, requesters can call the BJA Clearinghouse. The BJA Clearinghouse, a component of the National Criminal Justice Reference Service (NCJRS), shares BJA program information with state and local agencies and community groups across the country. Information specialists are available to provide reference and referral services, publication distribution, participation and support for conferences, and other networking and outreach activities. The Clearinghouse can be reached by:

❒ **Mail**
P.O. Box 6000
Rockville, MD 20849–6000

❒ **Visit**
2277 Research Boulevard
Rockville, MD 20850

❒ **Telephone**
1–800–688–4252
Monday through Friday
8:30 a.m. to 7 p.m.
eastern time

❒ **Fax**
301–519–5212

❒ **Fax on Demand**
1–800–688–4252

❒ **BJA Home Page**
www.ojp.usdoj.gov/BJA

❒ **NCJRS World Wide Web**
www.ncjrs.org

❒ **E-mail**
askncjrs@ncjrs.org

❒ **JUSTINFO Newsletter**
E-mail to listproc@ncjrs.org
Leave the subject line blank
In the body of the message,
type:
subscribe justinfo
[your name]

BJA

BJA World Wide Web Address

**For a copy of this document online,
as well as more information on BJA,
check the BJA Home Page at
www.ojp.usdoj.gov/BJA**

U.S. Department of Justice
Office of Justice Programs
Bureau of Justice Assistance

Washington, DC 20531

Official Business
Penalty for Private Use $300