STATE OF ALASKA

ALASKA JUDICIAL COUNCIL

PLAN FOR THE INTEGRATION OF ALASKA'S CRIMINAL JUSTICE COMPUTER SYSTEMS AND THE CREATION OF A COMPREHENSIVE CRIMINAL HISTORY REPOSITORY

MAY 2, 1994

WOLFE & ASSOCIATES, INC.
5325 WYOMING BOULEVARD, N.E.
ALBUQUERQUE, NEW MEXICO 87109
(505) 821-9336

Acknowledgments

We wish to acknowledge the valuable contributions and assistance of individuals from the many agencies who shared their time and expertise in responding to our questions and requests for information and materials. We are very appreciative for their assistance and wish to extend our thanks for professional services and personal courtesies. Special thanks are extended to Mr. William T. Cotton, Executive Director, Alaska Judicial Council, and his staff for their cooperation and assistance in facilitating agency interviews, hosting meetings with criminal justice committees, and gathering important documents. We also wish to thank agency administrators and their staffs for their tireless and generous contributions--specifically, Mr. Kennneth E. Bischoff, Director, Administrative Services, Alaska Department of Public Safety; Mr. John Valensi, Director, Division of Information Services; Mr. Dean Guaneli, Assistant Attorney General, Criminal Division, Department of Law; Mr. Frank Prewitt, Commissioner, Department of Corrections; Dr. Allan Barnes, UAA Justice Center; and Mr. Arthur Snowden, Administrative Director, Alaska Court System.

We also wish to comment on the spirit of cooperation everywhere in evidence in all of the agencies we visited, and the dedication of the individuals in those agencies to make an integrated justice system a reality.

Table of Contents

Executive Summary

In 1993, after recognizing the inadequacies of Alaska's criminal justice computer information systems, the Legislature directed the Alaska Judicial Council to work with the criminal justice agencies to improve the operation and coordination of these computer information systems. The Council contracted with independent consultants Wolfe & Associates to review Alaska's current systems and present a comprehensive plan for improvements.

This report shows how Alaska can create effective and coordinated criminal justice information systems in the next five years. The plan takes advantage of Alaska's existing investment in mainframe computers as well as newer technologies to suggest a cost-effective and practical approach that retains the investment in existing mainframes during a phased migration to a smaller, more cost-effective computer architecture. This plan to improve the quality and availability of criminal justice information in Alaska identifies the issues that must be resolved, presents recommendations for creating a comprehensive criminal history record repository, and provides alternative technical solutions for integrating criminal justice information systems.

We recommend that the legislature and agencies take the following four crucial steps immediately:

1. **The legislature should pass the APSIN legislation (HB 442 and SB 321) which will require fingerprinting of criminals, improve the collection of criminal justice information, and establish a framework for agency coordination.**

2. **The legislature should immediately fund the Department of Corrections ($150,000) and the Department of Law ($75,000) to begin planning to replace their outdated and inadequate computer information systems. These departments, especially DOC, must commit adequate and skilled personnel to this planning process if it is to succeed.**

3. **The Department of Public Safety must develop a plan for a new fingerprint system and must purchase more efficient live-scan fingerprint devices. The legislature should fund these purchases in its 1995 session.**

4. **The Department of Administration must begin to implement a multi-protocol communications backbone network for all state agencies. It must develop a capital budget request to the 1995 legislature to complete this project. The legislature should give funding of this backbone network the highest priority.**

A. Summary of Findings

Our findings confirm what the legislature understood when it ordered this project: criminal justice computer information systems in Alaska are, to varying degrees, inadequate even for individual departments. The state designed and acquired many parts of the systems twenty or more years ago, when the demographics, state structure, prison population and technology all were vastly different from the situation in 1994. The various departments' systems, even when adequate for their individual needs, seldom can communicate with one another. This inability to communicate leads to inefficiency, duplicative costs and numerous mistakes that cost the state money and threaten public safety. The departments have made recent efforts to work together, but substantial problems remain.

1. The criminal justice computer information systems are, to varying degrees, inadequate even for individual departments.

While the Department of Public Safety's computer information system best serves the needs of its department, even this system needs improvements. Specifically, DPS needs a new fingerprint identification system. The Court System's information system is comprehensive in theory; however, the software is only now being written. The Department of Law's system is outdated and not as useful as it should be.

The Department of Corrections is in the worst position with a computer system that dates back over twenty years. It must manage a large and expanding prison population, as well as a budget well over $100,000,000 per year, with what is essentially a paper information system. The great expense and chance for serious mistakes created by managing such a complicated organization without an adequate computer information system makes a compelling case for implementing the systemwide changes we suggest.

2. The Departments' computer systems are not coordinated.

Many, though not all, of the subparts of Alaska's criminal justice computer systems should work together. Each department processes the same criminals, collects much of the same information about them, and in many cases desperately needs information available only from other agencies. Nonetheless, the departments have separate systems that for the most part do not communicate.

An important example is the typical fate of information about an offender's conviction. Ideally, the court would immediately enter the conviction into a court case management computer system and transfer it electronically to Corrections, Public Safety, Prosecutors, and the Public Defender Agency. Instead, court clerks write this essential conviction information onto paper forms and send it with varying degrees of speed and efficiency to other agencies. Workers at the other agencies then must manually type the information into the various computer systems, sometimes months later, with the data entry errors that accompany manual systems.

3. The criminal justice agencies are working together to improve the system.

All agencies are participating in interagency groups designed to identify critical integration issues and resolve them. The Criminal Justice Working Group, the Computer Policy Coordination Group, and the Criminal Justice Information Systems Technical Users Group meet regularly, with staff support from the Alaska Judicial Council. The Department of Administration, Division of Information Services has defined the requirements for and is working to implement a statewide backbone telecommunications network that would allow agencies using different computer systems to communicate with one another. The Alaska Court System has spent three years designing a state-of-the-art case management system. The Department of Public Safety has significantly improved the identification of offenders and has provided leadership in implementing change.

4. Unless improvements are made, Alaska faces substantial and increasing problems.

Inadequate case management systems severely compromise many important functions of Alaska's criminal justice system. Under the current system, child care centers and other employers do not have the complete, accurate and reliable criminal history records needed to identify convicted child molesters and felons who apply for jobs. State social service agencies do not have the complete, accurate and reliable criminal history records needed to screen out convicted felons from foster care and other programs. Judges, prosecutors and defense attorneys cannot accurately apply presumptive sentencing guidelines because the state cannot create the offender's full criminal history. Other important state legislation, such as the "three strikes and you're out" initiative and sex offender registration, cannot be implemented without accurate, timely and complete criminal history records. The inadequacies of the current systems also compromise victims' rights, because the systems often cannot notify victims of the release of offenders from state custody.

While the Department of Public Safety has significantly improved identification processing, the inadequacy of the state's current fingerprint identification system compromises Alaska's ability to identify felons who could otherwise avoid detection by using an alias. Also, a new fingerprint identification system is needed in order for the state to fully comply with important federal programs such as the Brady Bill, the Child Protection Act, the interstate exchange of criminal history records, and the convicted alien reporting program of the Immigration and Naturalization Service (INS).

B. Platform Choices

The plan examines three possible technical system configurations that would permit all the criminal justice agencies' operating systems to share information. Collectively, the three technical alternatives encompass the range of computer resources available in the industry, from the desktop to the mainframe. While all would enhance the ability of individual state systems to share information and create a useful and timely criminal history record, they differ in their degree of technical complexity, costs, and impact on the agencies' administrative and personnel resources. We recommend that the state move, over the next five years, from the mainframes to client/server technology.

We believe Alaska will benefit most from a migration to a client/server computing platform because it maximizes the investment in the current mainframe technology, while moving judiciously to a smaller, more effective computer platform. This alternative calls for the state to move in phases away from the mainframe to client/server. The mainframe still will serve as a data repository and as the current platform for complex mission critical applications. New applications will be developed on client/server technology, and the state will begin moving existing applications from the mainframe to the new technologies. Serious administrative problems most likely would attend a too-rapid conversion to client/server technology. The open server concept accommodates all new, heterogeneous systems developed to take advantage of client/server technology.

Businesses describe this approach as "rightsizing." Rightsizing puts the right part of an application on the right computer. For example, that part of the criminal history record that the users interact with would be put on the client PC, while the data that comprise the criminal history record would stay on the mainframe. It represents an appropriate division of labor in an essentially "open computing environment"--the PC's run the application from the desktop, a small but robust Unix server brokers information requests and handles sophisticated transactions, and the mainframe uses its large capacity to house the data and to run the more complex operations.

Perhaps the most significant advantage of this gradual approach is that it gives the state some time to wait for the new client/server technology to mature. In the next two years, refinements in client/server technology will ensure data integrity and security in transaction processing. Other advances will ensure that the technology fully meets the state's processing requirements. This plan lets the state move away from the mainframe as resources and budgets permit.

C. Summary of Recommendations

Part 2 of this report discusses our recommendations in detail. In particular Chapter VIII sets out a five-year implementation plan for each department. A summary of recommendations appears here.

1. The legislature should enact the proposed APSIN legislation to improve criminal justice information.

At the heart of any criminal justice information system is accurate identification of offenders and tracking of important case "events" (i.e., arrest, release, conviction, sentence, etc.). Current Alaska statutes do not mandate fingerprinting of felons or misdemeanants, nor do they require criminal justice agencies to report important case "events" to the criminal history repository. The legislature and governor have worked together during this session on legislation to remedy these fundamental problems. The bill provides the framework for the success of any integration efforts. (The proposed APSIN legislation requires fingerprinting for all felonies immediately, and for all misdemeanors by 1996. This legislation also establishes authority with the Commissioner of Public Safety, advised by a board consisting of representatives from interested agencies, to require the criminal justice agencies to submit arrest and disposition information. See Appendix C for a discussion of the proposed legislation).

2. The legislature should enact the proposed APSIN legislation to support criminal records by fingerprints.

The state must positively identify offenders in order to maintain accurate criminal history records. Fingerprints remain the most widely accepted method of verifying an offender's identity, yet Alaska routinely identifies *only thirty-nine percent* of the offenders in the criminal history repository through fingerprints. The proposed legislation will solve this problem by requiring that agencies submit fingerprint cards for all offenders to the Department of Public Safety (currently, such submittals are voluntary.)

3. The legislature should fund a new automated fingerprint system, including Live-Scan fingerprint devices in the Department of Public Safety.

The second step in establishing a criminal history records system, after giving DPS the authority (discussed above) to require fingerprinting, is to provide the means of acquiring and using fingerprint records. The current fingerprint system cannot hold even the fingerprints that are anticipated in the near future. DPS must analyze its needs and present a funding request to the legislature for its 1995 session.

The funding request also should include live-scan devices for taking fingerprints easily, accurately and in a cost-effective manner. Department of Health and Social Services should have live-scan devices to fingerprint juvenile offenders as well.

4. The Department of Corrections must begin now to plan and acquire a computer information system to efficiently administer the department.

The Department of Corrections desperately needs a computerized management system to efficiently run the Department. The legislature this year should fund the detailed, methodical planning process needed before the department acquires a new system. Chapter IV explains the details of this planning process.

In addition to having funds for the planning process, DOC must make a commitment to carry it out. The Department must assign a capable administrator with some technical understanding of the project to lead the effort, and must authorize this person to call on Corrections personnel at all levels to participate in planning and implementation.

5. The Department of Law must begin to plan for the acquisition of a new case management system.

While DOL's situation is not otherwise analogous to DOC's, DOL does need to plan for and acquire a new case management system. DOL should work closely with DPS in this process. The design process that both DOL and DOC choose must include representatives of all other criminal justice agencies so that the systems that meet the agencies' individual needs also serve the needs of the justice system as a whole. See Chapter IV for more details.

6. The legislature should support the efforts of the other departments to improve their computer information systems.

This recommendation is the highest priority for the departments of Law and Corrections, because they have the least functional systems. Other agencies, such as the Alaska Court System and the Public Defender Agency, are using existing funds to develop case management systems using newer technologies. The legislature should support their continuing efforts. Even DPS, which has the most advanced system and can accommodate the electronic transfer of criminal history and offender information, needs further improvements.

7. Acquire a multi-protocol backbone network.

The Department of Administration, Division of Information Services (DOA/DIS) should receive capital funds to acquire a multi-protocol network. Because computers cannot communicate without a network, the network is critical to the successful integration of the criminal justice information systems.

8. Improve the quality of criminal history information

The criminal justice agencies as a whole must improve the mechanisms for arrest and disposition reporting. While DPS promptly enters into its computers all the fingerprints, arrest information, and court judgments that it receives, many fingerprints are never submitted and many are not even taken; all arrests are not entered by the law enforcement agencies; and some court dispositions are not received by Public Safety. Also, vital information on the location of the offender is not available from the Department of Corrections.

9. Comply with federal initiatives.

Several federal initiatives will require the state to provide complete, accurate, and timely criminal history records. The current lack of fingerprint-supported records and the inadequacy of criminal records restrict the state's ability to comply with these initiatives.

10. Develop standards for information sharing

Technology standards for information sharing represent the infrastructure that allows different computer systems to communicate effectively. Interagency committees already have set standards for key data elements, such as arrest tracking number (ATN), person ID number, name, social security number, date of birth, and court case number. These committees must continue to meet to resolve the questions of interfacing and new technology standards.

11. Expand the contents of the criminal history record.

The contents of the criminal history record maintained by the repository should be expanded to meet the real needs of the users of the records. The repository must store more data elements, and must make its information easily accessible. For example, implementing the "three strikes and you're out" initiative will require a criminal history record that tracks and records dispositions by charge and count.

12. Establish policies for interagency coordination.

Some organization must lead the way in addressing policy issues, standards, and integration methods. This agency also should provide leadership in coordinating technical efforts related to sharing information among justice agencies. The Criminal Justice Working Group, composed of cabinet-level officials from the operational agencies is the appropriate organization to resolve interagency policy issues relating to information sharing. The Department of Public Safety and the Telecommunications Information Council (TIC) also have leadership roles to play. See Chapter III for more discussion.

13. Enhance the criminal history repository.

Chapter VI of this plan describes the additional pieces of information that agencies should send to the criminal history data base. These enhancements should be carefully considered and implemented as new technologies provide a way to deliver the data.

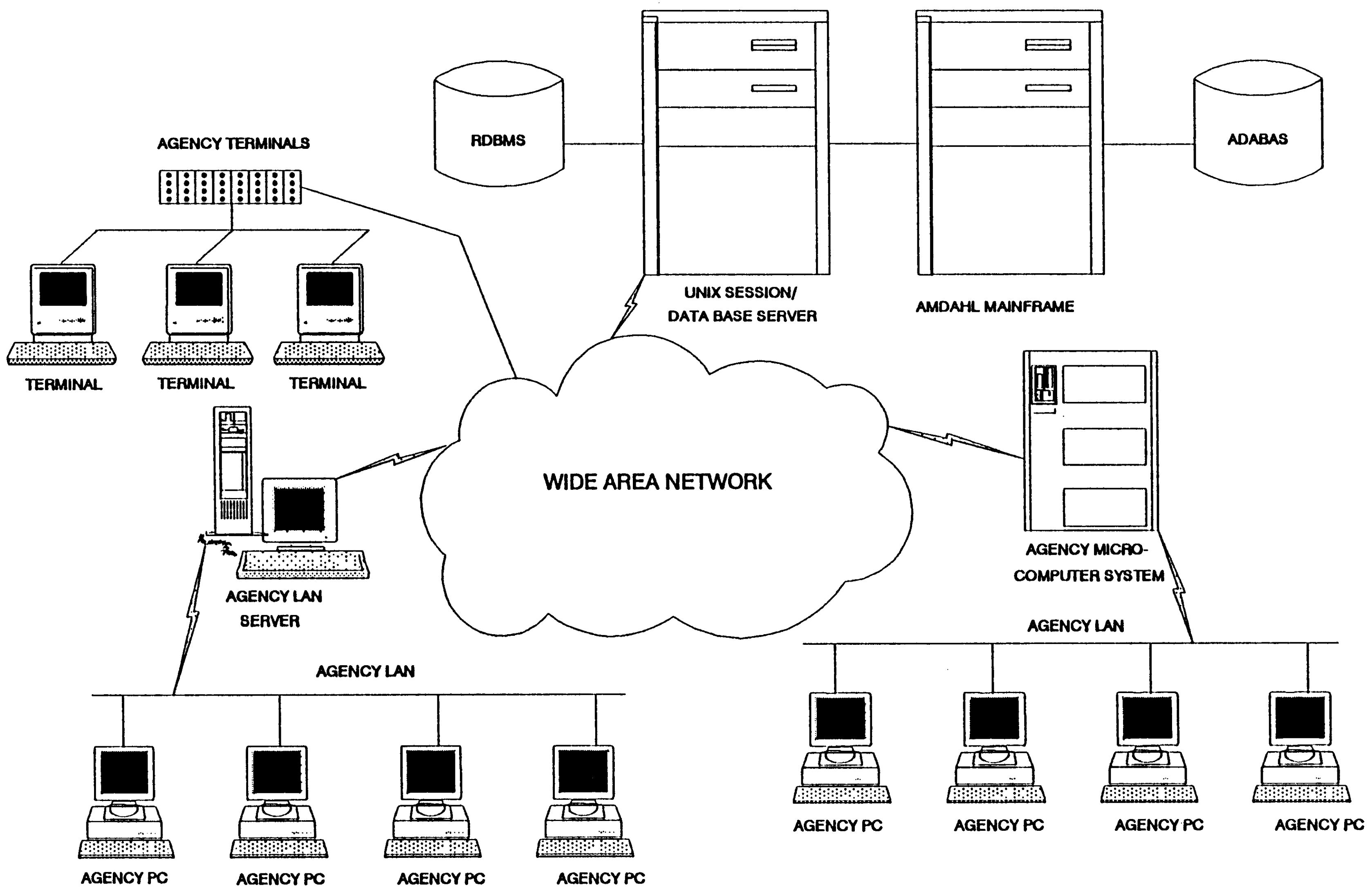
14. Integrate agency systems.

Once the Alaska Court System and the departments of Law and Corrections have new computerized case management systems, they must transfer data electronically to the criminal history repository. Electronic transfers of key data among agency systems reduce data entry duplication and chances for errors.

15. Implement recommended technical alternative.

The recommended architectural alternative, shown as Figure 1 and discussed in Chapter VII, combines client/server technology with mainframe processing. All agencies should develop new systems using the "open" architectures offered by client/server systems.

FIGURE 1
ALTERNATIVE 3
UNIX SESSION/DATA BASE SERVER WITH RDBMS/
MAINFRAME DATA BASE SERVER WITH ADABAS



16. Establish standards for information sharing.

DOA/DIS should chair the process of developing the open systems standards discussed in Chapter III and Appendix D. Standards ensure compatibility of new "open" systems among agencies. DIS also should assist agencies in evaluating how to use these new technologies. DIS should help agencies to select the best data base and assorted tool sets for their applications. The criminal justice inter-agency committees should develop standards for the transfer of criminal justice data among systems and the methods by which this transfer will occur.

D. The Cost of the Master Plan and the Cost of Doing Nothing

We estimated that Alaska spends about $300 million a year on its criminal justice system—about $1.5 billion over the next five years. The steps outlined in this report will cost about $16,880,000 over the next five years, about one percent of total spending on the system. These costs are set out in detail in Chapter VIII. We believe they will lead to savings far greater than the costs.

Given the current fiscal climate in Alaska, the legislature and justice agencies will be tempted to reject the steps set out in this report, instead doing nothing and hoping that the current criminal justice computer systems will suffice. This alternative is neither realistic nor without cost. The $300 million Alaska spends on criminal justice every year includes the unnecessary costs of duplicate data entry, and a myriad of time-consuming manual tasks that other jurisdictions have automated. The inefficiencies in just Department of Corrections, not to mention the system as a whole, are staggering. Without an integration of criminal justice information, the state of Alaska will continue to pay a high price for information that is neither accurate, timely, nor available.

If the state does nothing to coordinate and integrate its criminal justice computer systems, the justice agencies will require large numbers of additional staff to manually generate complete and accurate information. As the existing equipment ages further, the state will spend ever-larger amounts to maintain obsolete technology. Investing money in Alaska's justice agencies' case management systems will automate the collection, maintenance, and dissemination of criminal history record information and generate the information needed to administer justice and improve public safety without requiring large numbers of additional staff. Further, without the improvements outlined in this report, Alaska cannot comply with new federal and state mandates, let alone existing state laws.

Nor can the state address deficiencies found in a single agency and ignore the rest of the criminal justice agencies. The deficiencies we found exist throughout the criminal justice system, and the system as a whole depends on many different agencies to provide complete, accurate, and timely information about crime and offenders. The solution, therefore, must include the entire system.

E. The Contents of the Report

This Executive Summary represents only the highlights of our findings, technical alternatives, and recommendations. The remainder of the report provides a complete discussion of these and other topics. The specific chapters that follow include:

- **Chapter I: Description of Existing Situation** -- This chapter describes agencies' existing systems, discusses the adequacy of those systems for meeting agency needs and for sharing information with other agencies, and outlines agencies' future technology development plans. This chapter also discusses agencies' readiness for integration.

- **Chapter II: Information Quality Assessment** -- This chapter assesses the quality of the existing criminal history data.

- **Chapter III: Need for a Policy Framework to Develop State Information Technology** -- This chapter discusses the need for a policy framework for developing information technology, including the need for a policy-making body and a lead agency to coordinate integration activities.

- **Chapter IV: Business Process Re-engineering** -- This chapter explains the business assessment and design process that agencies should undertake before acquiring new systems.

- **Chapter V: Model for an Integrated, Computerized Criminal History Record** -- This chapter discusses the criminal history record and how it should be used to meet both state and federal criminal history information needs.

- **Chapter VI: Criminal History Record Data Elements** -- This chapter lists and discusses the specific data elements that should be contained in a criminal history.

- **Chapter VII: Alternative System Configurations** -- This chapter explains the trends in technology, suggested client/server standards, and the alternatives for future system evolution. It also presents our recommended system configuration for Alaska.

- **Chapter VIII: Implementation Plan** -- This final chapter presents the detailed five-year implementation plan through which Alaska can achieve coordinated criminal justice information systems and high-quality criminal history records.

- **Appendix A** This part summarizes literature pertaining to integrating criminal justice systems and updating the criminal justice repository.

- **Appendix B** This part describes the operational structure of the Division of Information Services.

- **Appendix C** This part contains our commentary on the proposed APSIN fingerprint legislation.

- **Appendix D** This part sets out recommended open systems standards for Alaska.

Chapter I

Description of the Existing Situation

A. Introduction

The Alaska Legislature appropriated to the Alaska Judicial Council funds to develop a General Design for Integrated Criminal Justice Information Systems in Alaska. The Legislature intended that the plan would help it effectively manage and expend funds for new criminal justice system efforts. The Alaska Judicial Council facilitated a series of meetings with agency representatives to discuss ways to better coordinate information systems. The Council, working with the criminal justice agencies, also prepared an RFP for professional consulting services to assist in developing a "plan for the integration of criminal justice computer systems and the creation of a comprehensive criminal history repository."

Wolfe & Associates worked from December 20, 1993 through April 29, 1994 to complete the system design. The consultants reviewed thirty-five documents, ranging from federal publications to reports on agency status and planning efforts, conducted forty-nine interviews with representatives from all of the operational agencies affected by an integration effort, and developed technical alternatives based on the findings from the literature and these interviews.

This General Design for an Integrated Criminal Justice Information System in Alaska is a set of strategies and technology alternatives for improving the quality and availability of criminal justice information. We commend the legislature for its concern about the quality of criminal justice information, and for its leadership in addressing this problem. Other states and the federal government share these concerns.[1] U.S. Attorney

[1] The Attorney General recently stated that:

> It is all too easy to forget how often we need to know a person's criminal history. When bond is set in a criminal case, the defendant's criminal history may indicate whether there is serious risk of flight. When a judge goes to sentence an individual convicted of a crime, that judge is entitled to know the past criminal behavior of the person standing before the bench. When our government is trying to decide whether an individual can be trusted to have access to our nation's miliary secrets, a history of

General Janet Reno recently assessed the nation's ability to use criminal history records to identify criminals, administer justice, and protect the public as "abysmal."[2] She noted that of the 53.3 million criminal records in state repositories, only 17.5 million (or 33%) are available on the FBI's Interstate Identification Index (III), and only 9.2 million (or 17%) of the records are supported by conviction information.

The Attorney General and the state's legislature point to the same deficiency in Alaska's criminal history record computer systems: the state's current technologies do not provide accurate, complete, and timely criminal history information.

This chapter describes in detail each criminal justice agency's information needs, resources available to meet those needs, the technologies (hardware and software) currently used to fulfill those needs, and future technology plans. Much of the information in this chapter builds on the results of in-depth structured interview sessions with key agency representatives.[3] This chapter is organized by agency.

B. Department of Administration, Division of Information Services (DIS)

1. Information Needs and Resources of DIS.

The Division of Information Services provides shared-use, centralized data processing, data communications, and telecommunications services to state and other government agencies. DIS also staffs three information technology interagency

> criminal behavior may shed light on that question... In various states, criminal background checks are done before individuals may e hired as bank tellers, day care workers, retirement home aids, and school bus drivers. (National Conference on Criminal History Records: Brady and Beyond, February 9, 1994).

[2] "Given the new miracles of technology which emerge everyday, our current ability to conduct reliable background checks is abysmal."

[3] The interviews addressed four topics: administrative and policy issues, information requirements, technical issues and resource availability. Administrative/policy issues included information systems planning, roles and responsibilities, supporting legislation, resource adequacy and standards. Information requirements involved issues such as information sharing, information needs, constraints, workflow process and backlogs. Technical issues involved technical problems related to information sharing, communication networks, new application requirements, and current technology platform architectures. Finally, resource availability discussed issues that impact agency resources, including hardware, software, personnel and budgets.

organizations on a rotating or as-needed basis.[4] The governor chairs the cabinet-level Telecommunications Information Council. Representatives from the legislative and judicial branches, as well as one public member appointed by the governor make up the Telecommunications Information Council.[5] The Council provides policy direction for the Information Systems Committee and the Information Systems Project Review Committee.

The Information Systems Committee is an interagency group of information system managers. It provides recommendations to the Commissioner of Administration on policies and procedures for DIS's centralized computing and telecommunications facilities. It also serves as the primary distribution point for information relating to DIS activities.

The Information Systems Project Review Committee is an executive-level review body which reports to the Commissioner of Administration. The committee's task is to implement a centralized review mechanism above the departmental level to offer state agencies a peer-level appraisal of their information systems and telecommunications projects. Members include one representative each from the Office of Management and Budget and DOA's Divisions of Information Services and General Services. Two other department representatives serve on a rotating basis.

To handle all its responsibilities, DIS is divided into three sections: Computer Services, Customer Services, and Administrative and Telecommunications Services. Each section in turn is divided into two or more units.[6] The three sections and their component units are discussed in detail in Appendix B.

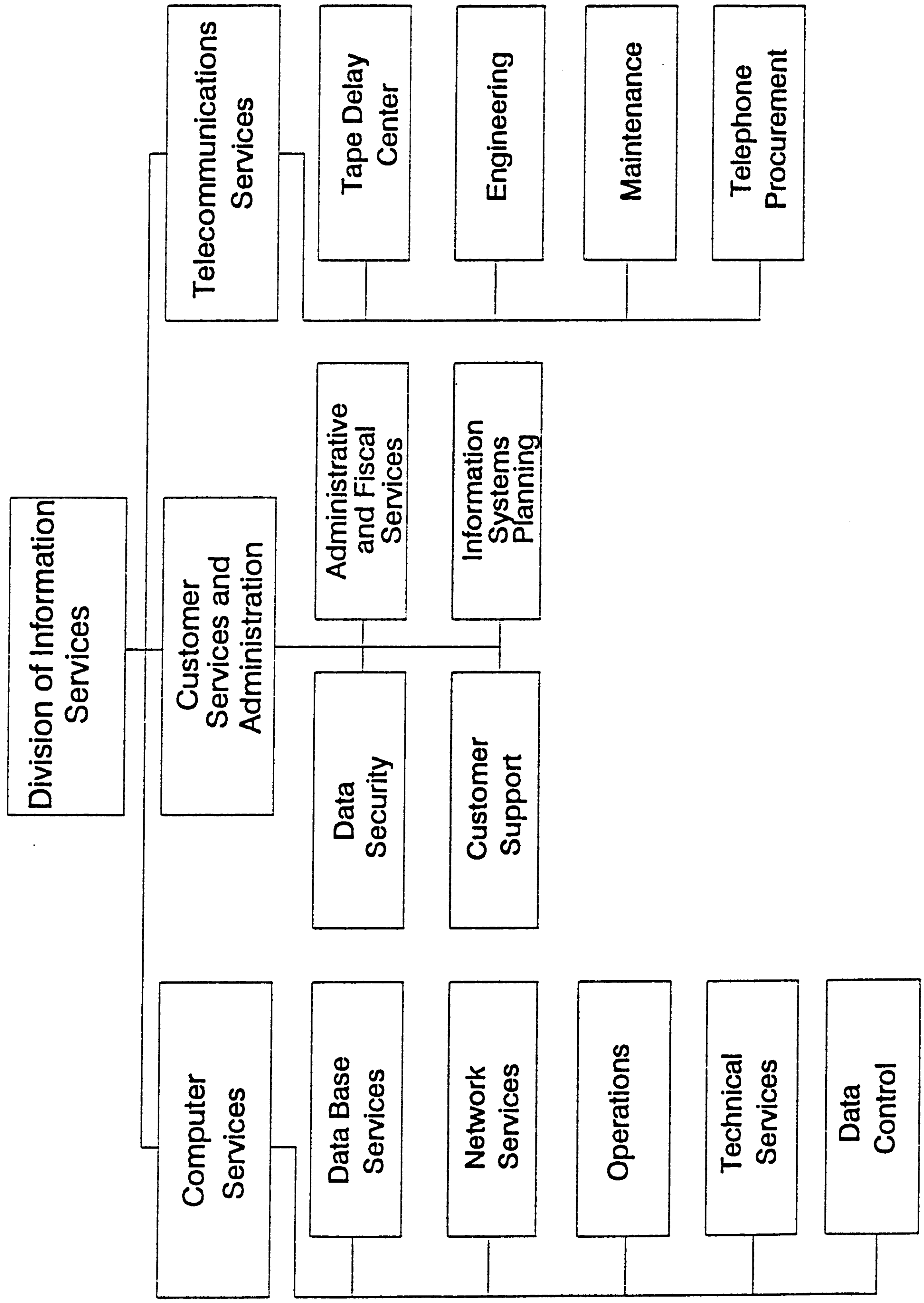
[4] These three organizations are: the Information Systems Committee (ISC), the Information Systems Project Review Committee (ISPR), and the Telecommunications Information Council (TIC). The ISC was established in 1983 by the governor to ensure the effective management of information resources. The ISPR was established in 1991 by the governor to review agencies' information systems and telecommunications projects in order to avoid redundant or inappropriate purchases. The TIC was established in 1987 by the Legislature to ensure the effective management of information resources at the policy level by establishing short-term plans for data processing and telecommunication needs, and for establishing guidelines for public access to information.

[5] Due to the large membership of the Council, a smaller, more manageable Executive Committee was formed in 1992. The Executive Committee is chaired by the Commissioner of Administration.

[6] Figure 2 is a division organization chart. The responsibilities of each division are detailed in Appendix B.

FIGURE 2

DIVISION OF INFORMATION SERVICES



2. *Overview of Existing Technology.*

To meet agencies' varying data communication needs, DIS currently runs two networks: a System Network Architecture (SNA) and a Wide Area Network (WAN). The state mainframe uses the System Network Architecture. The Department's current system architecture is summarized in Figure 3.

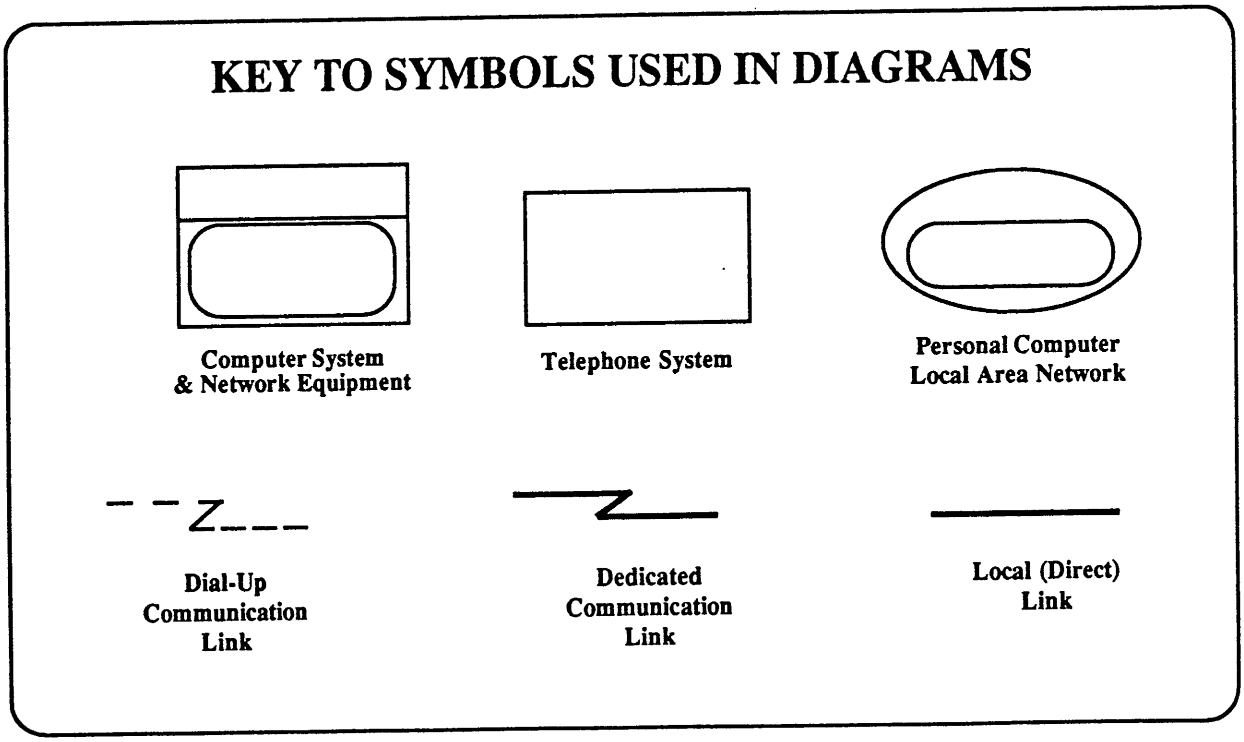
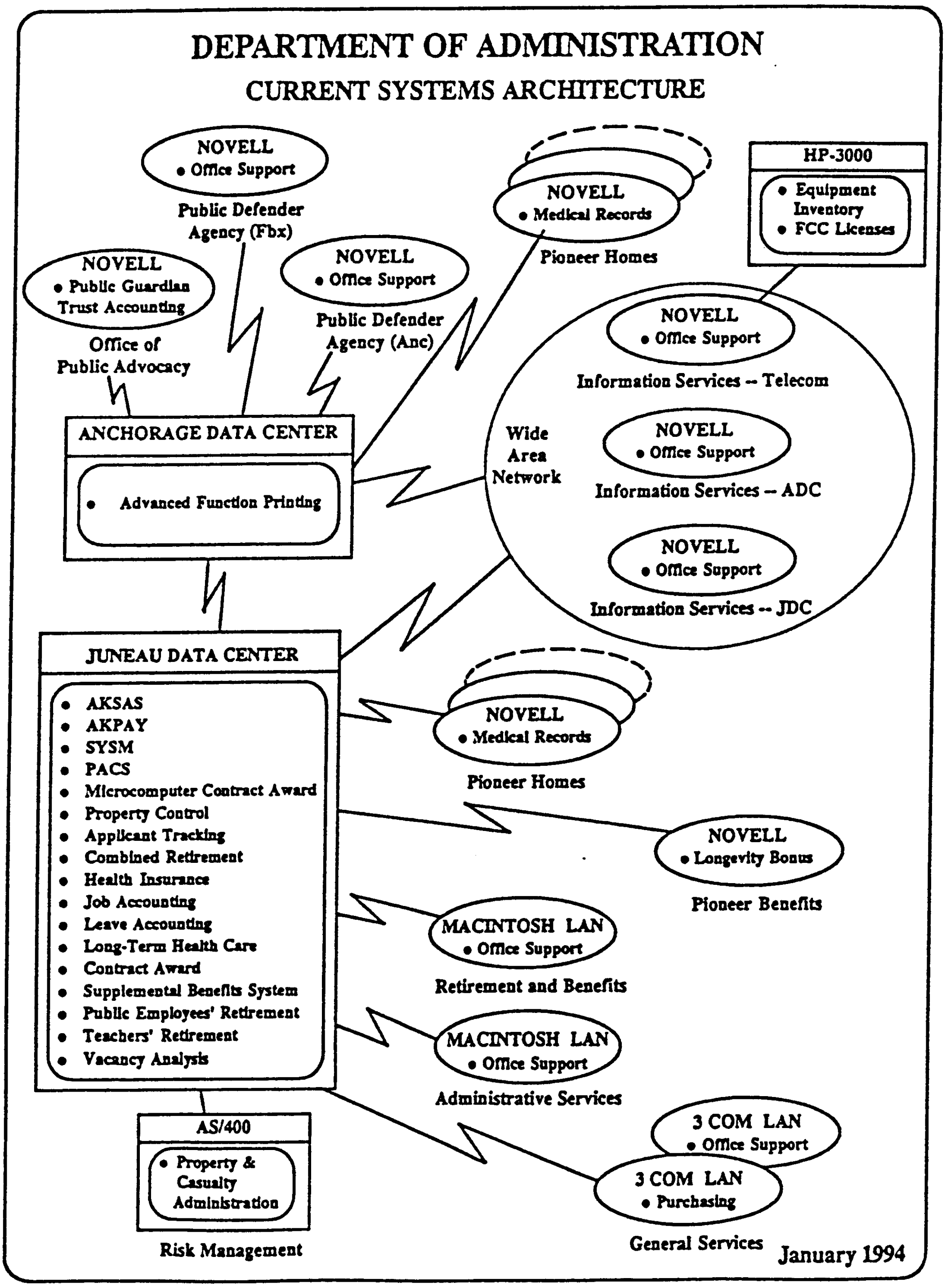

KEY TO SYMBOLS USED IN DIAGRAMS
Computer System & Network Equipment
Telephone System
Personal Computer Local Area Network
Dial-Up Communication Link
Dedicated Communication Link
Local (Direct) Link

FIGURE 3

INFORMATION SYSTEMS DIAGRAMS



Alaska 1994 Information Management Plan

Appendix F.7

19/6/2SYSTEMS.PMS/7—2/94

DRAFT

a. The SNA

From a statewide data network begun in 1972, DIS has grown to provide on-line access to applications located on the mainframe computers in Juneau, Anchorage, and Fairbanks. The mainframe network has over 300 communications lines disseminating from its three hubs. Designed specifically to be able to connect remote terminal devices, the mainframe connects over 7,000 terminals located in thirty-six cities around the state.

DIS operates two major data centers, one in Anchorage and the other in Juneau.[7] They are connected via the systems network architecture (SNA) network.[8] The three major network nodes are in Juneau, Anchorage, and Fairbanks. The Juneau node includes the Juneau Data Center and services southeast Alaska and the Lower 48. The Anchorage node includes the Anchorage Data Center and services southcentral Alaska, IBM-IN, the National Law Enforcement Telecommunications Network (NLETS), and the National Crime Information Center. The Fairbanks node includes the University of Alaska's administrative computing system, and services the data processing needs of northern Alaska communities. A data communications network connects the centers with communities throughout the state.[9]

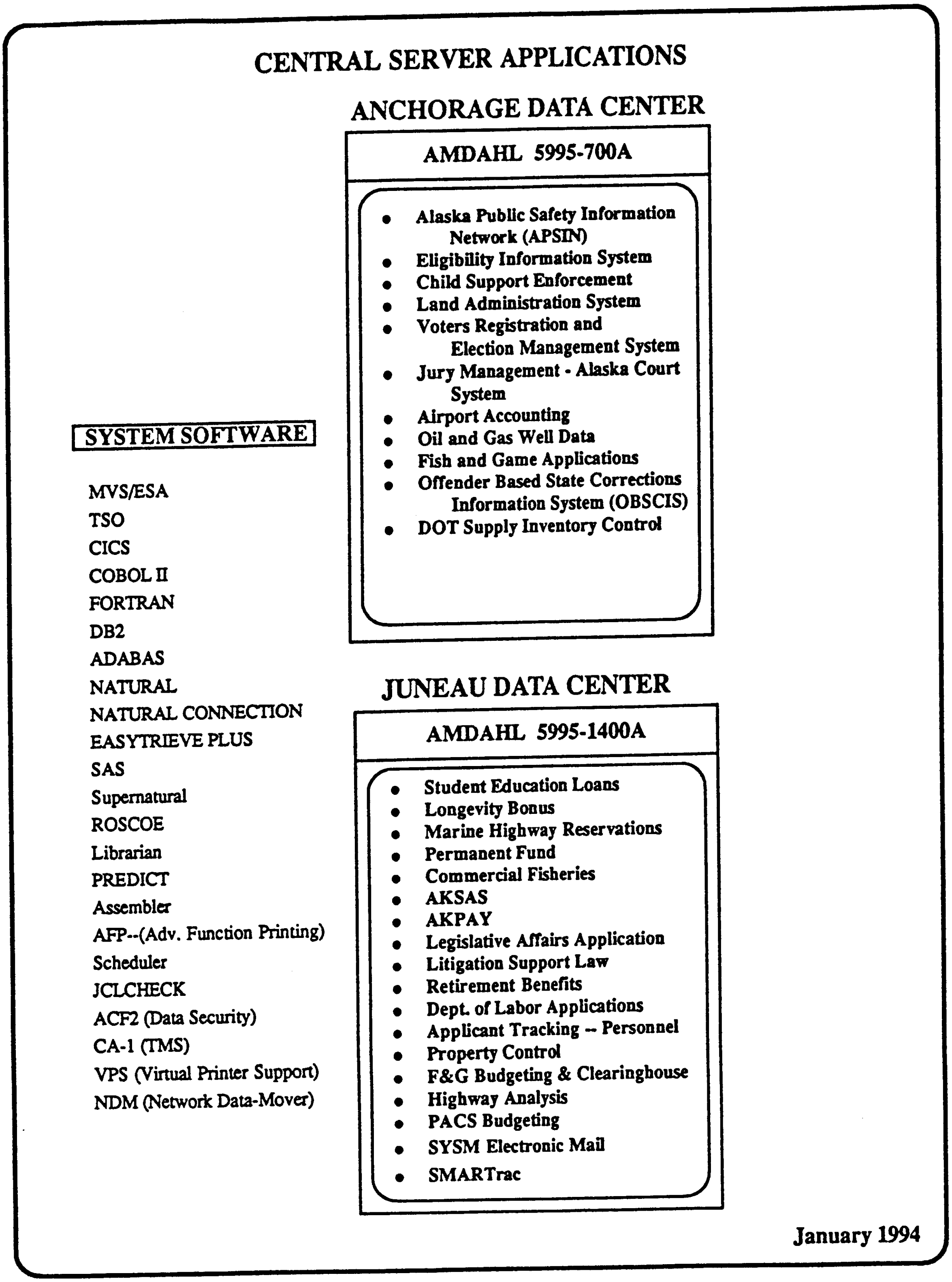
[7] Two mainframes are the heart of the data centers: an Amdahl 5995-700A at the Anchorage Data Center and an Amdahl 5995-1400A computer at the Juneau Data Center. Both computers utilize the MVS operating system. Figure 4 diagrams these information systems and lists the applications that reside on the two mainframes.

[8] Various non-criminal justice agency computers, i.e., University of Alaska, Legislative Affairs, IBM Information Network (IBM IN), and the Environmental Protection Agency, also are connected to the network. Figure 5 shows the statewide data network.

[9] Figure 6 shows the circuits that support the network. Over 200 different applications are processed by approximately twenty-four agencies on the mainframe computers located in Juneau and Anchorage.

FIGURE 4

INFORMATION SYSTEMS DIAGRAMS



CENTRAL SERVER APPLICATIONS

ANCHORAGE DATA CENTER

AMDAHL 5995-700A

- Alaska Public Safety Information Network (APSIN)
- Eligibility Information System
- Child Support Enforcement
- Land Administration System
- Voters Registration and Election Management System
- Jury Management - Alaska Court System
- Airport Accounting
- Oil and Gas Well Data
- Fish and Game Applications
- Offender Based State Corrections Information System (OBSCIS)
- DOT Supply Inventory Control

SYSTEM SOFTWARE

MVS/ESA
TSO
CICS
COBOL II
FORTRAN
DB2
ADABAS
NATURAL
NATURAL CONNECTION
EASYTRIEVE PLUS
SAS
Supernatural
ROSCOE
Librarian
PREDICT
Assembler
AFP--(Adv. Function Printing)
Scheduler
JCLCHECK
ACF2 (Data Security)
CA-1 (TMS)
VPS (Virtual Printer Support)
NDM (Network Data-Mover)

JUNEAU DATA CENTER

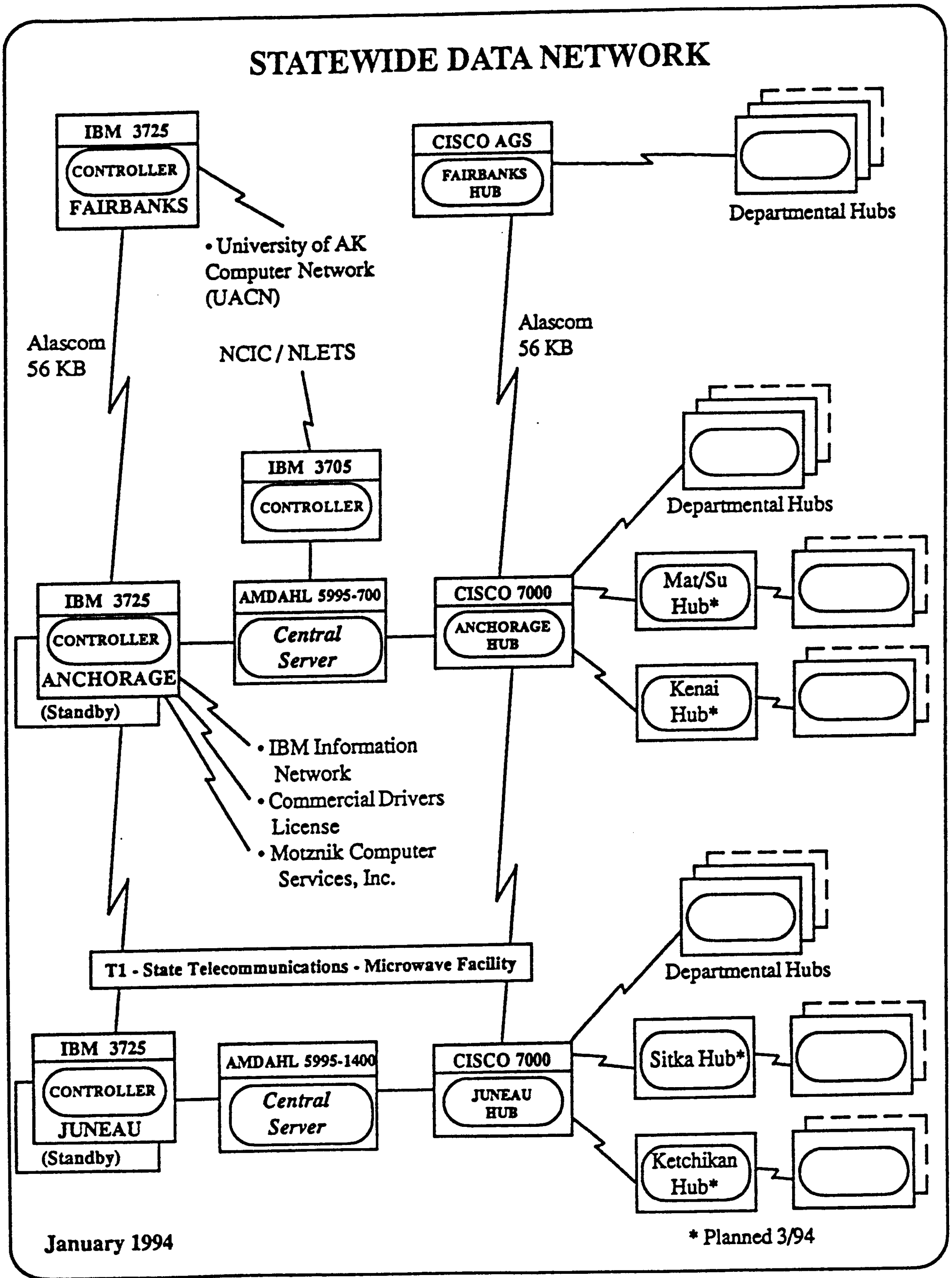
AMDAHL 5995-1400A

- Student Education Loans
- Longevity Bonus
- Marine Highway Reservations
- Permanent Fund
- Commercial Fisheries
- AKSAS
- AKPAY
- Legislative Affairs Application
- Litigation Support Law
- Retirement Benefits
- Dept. of Labor Applications
- Applicant Tracking -- Personnel
- Property Control
- F&G Budgeting & Clearinghouse
- Highway Analysis
- PACS Budgeting
- SYSM Electronic Mail
- SMARTrac

January 1994

FIGURE 5

INFORMATION SYSTEMS DIAGRAMS



Alaska 1994 Information Management Plan

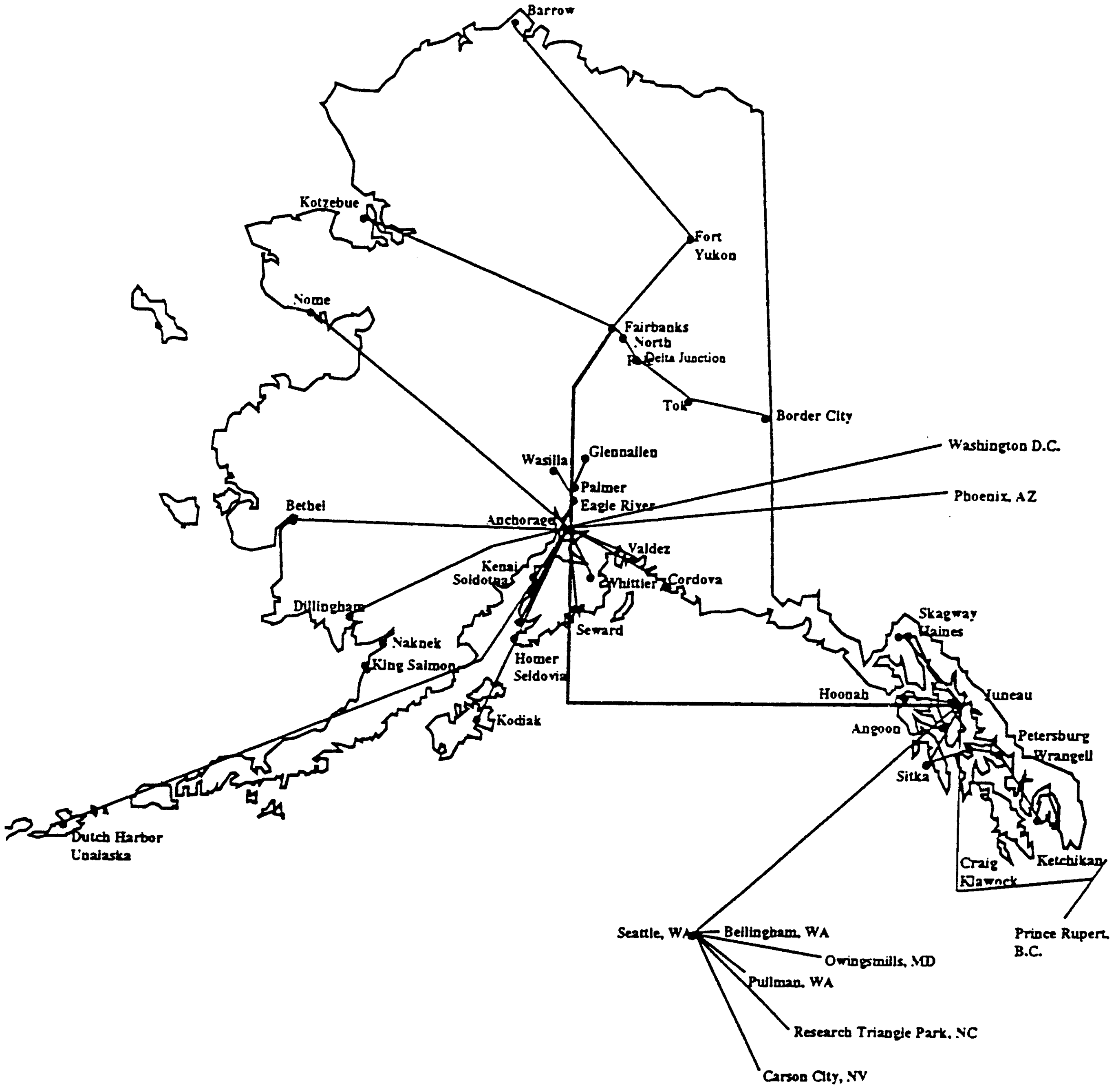
Appendix F.5

DRAFT

19/5/2SYSTEMS.PM5/5—2/94

FIGURE 6

STATE OF ALASKA DATA CIRCUITS



b. The Backbone WAN

Since 1990, DIS also has been supporting a wide area network (WAN) backbone service between Juneau, Anchorage and Fairbanks. The DIS backbone WAN, using CISCO multi-protocol routers located at the Anchorage and Juneau data centers, connects state LAN's in Anchorage, Fairbanks, and Juneau.[10] It provides connectivity to twenty LANs throughout Alaska. This connectivity is useful to agencies that have been installing midrange computer systems and then linking these computers together using local area networks (LANs), WANs and dedicated circuits. The DIS WAN also has InterNet addresses available to hook into national and international networks.

3. Future Technology Development Plans.

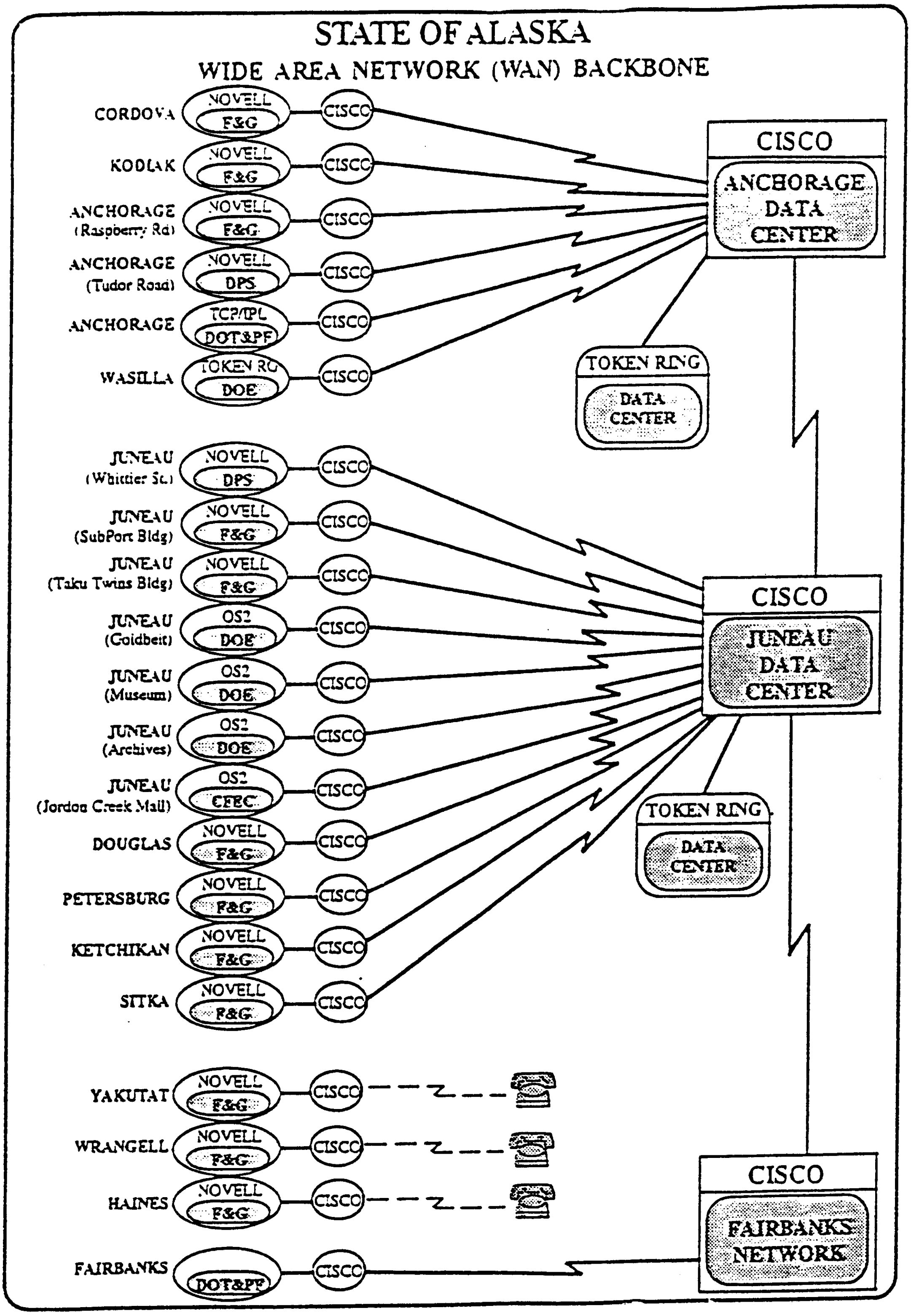
In 1993, DIS contracted with ALASCOM to define an architecture for a statewide internet (SWI) that would address the structure of LANs within individual departments and the WAN maintained by DIS, and also would integrate these networks with the current SNA network. ALASCOM recommended a multi-protocol statewide internet to consolidate all of the state's data networks into a single router-based network which would use public transmission facilities instead of dedicated circuits. This network could support client server or distributed processing, imaging, E-mail, and file transfers requiring a minimum bandwidth of 56 Kbs.[11] The one-time cost to develop the internet would be $3,250,000 over three years.

In addition to its continuing responsibilities with data centers and communications facilities, DIS's mission must grow as new technologies are developed and mature. DIS is the logical agency to help other state agencies avoid the confusion and potential inefficiency presented by the rapid development of new information technologies. For example, new technologies such as client servers, relational data bases, various tool sets and associated networks have been and are being introduced into the Alaska data processing user community. When acquiring these technologies in the future, agencies should be guided by uniform, comprehensive standards that would ensure connectivity, compatibility and proper use of these technologies. DIS and/or the

[10] Figure 7 shows how the LANs connect. Several other locations have dedicated connections.

[11] 56 Kbs is substantially above the predominately 9.6 Kbs equipment and facilities supporting the current network.

FIGURE 7


STATE OF ALASKA
WIDE AREA NETWORK (WAN) BACKBONE
CORDOVA
NOVELL
F&G
CISCO
KODIAK
NOVELL
F&G
CISCO
ANCHORAGE
(Raspberry Rd)
NOVELL
F&G
CISCO
ANCHORAGE
(Tudor Road)
NOVELL
DPS
CISCO
ANCHORAGE
TCP/IPL
DOT&PF
CISCO
WASILLA
TOKEN RG
DOE
CISCO
CISCO
ANCHORAGE DATA CENTER
TOKEN RING
DATA CENTER
JUNEAU
(Whittier St.)
NOVELL
DPS
CISCO
JUNEAU
(SubPort Bldg)
NOVELL
F&G
CISCO
JUNEAU
(Taku Twins Bldg)
NOVELL
F&G
CISCO
JUNEAU
(Goldbelt)
OS2
DOE
CISCO
JUNEAU
(Museum)
OS2
DOE
CISCO
JUNEAU
(Archives)
OS2
DOE
CISCO
JUNEAU
(Jordon Creek Mall)
OS2
CFEC
CISCO
DOUGLAS
NOVELL
F&G
CISCO
PETERSBURG
NOVELL
F&G
CISCO
KETCHIKAN
NOVELL
F&G
CISCO
SITKA
NOVELL
F&G
CISCO
CISCO
JUNEAU DATA CENTER
TOKEN RING
DATA CENTER
YAKUTAT
NOVELL
F&G
CISCO
WRANGELL
NOVELL
F&G
CISCO
HAINES
NOVELL
F&G
CISCO
FAIRBANKS
DOT&PF
CISCO
CISCO
FAIRBANKS NETWORK

TIC should lead the effort to establish these standards. In addition, the DIS should be prepared to provide operational support for large server equipment, help agencies select client server tools that meet their needs, and help agencies select the proper software or develop applications using these new tool sets. The role and responsibilities of DIS and the interagency organizations have been, and will continue to be, extremely important to the state.

C. Department of Public Safety

1. Information Needs and Resources of DPS.

The Department of Public Safety (DPS) uses computers to support data processing for its five divisions.[12] DPS also serves as the central repository for criminal history information. The Information Systems Section within the Division of Administrative Services provides all information-related services. The DPS Information Systems Section has ten professionals who support existing operations and develop new programs.

DPS collects criminal history information from other agencies and enters it into APSIN. Other agencies voluntarily submit arrest and disposition information to the DPS Records section. Arresting and booking agencies record information about their actions on the Criminal Case Intake and Disposition (CCID) form, as do prosecutors.[13] Courts mail information about final dispositions on written judgment forms.

Entering this data from other agencies into APSIN is time-consuming. None of the interfaces are automated at present.[14] The DPS Records and Identification Section enters disposition information from written judgment forms received from the courts. This unit

[12] The five divisions are: Alaska State Troopers, Motor Vehicles, Administrative Services, Fire Protection, and Fish & Wildlife Protection.

[13] Currently, about thirty-nine percent of the CCH records include positive identification of an offender through fingerprints.

[14] Although APSIN and the systems for the Departments of Law and Corrections all reside on the state mainframe, the systems are not compatible. The DPS systems use an ADABAS data base, while the departments of Law and Corrections' systems are batch-oriented, using COBOL and VSAM file structures. These latter two systems are difficult to modify. Efforts to add fields to assist in record matching is complicated by the old file structures and poor data quality. Until the departments replace those two systems, it will be difficult to have effective and accurate interfaces among all four criminal justice agency systems.

is understaffed, and is running 1,000 judgments behind per month. Their task is complicated by the lack of standardized judgments and the lack of consistent use of ATNs on the judgments. DPS also tracks CCID submittals manually, since no interfaces are automated. Staff time available for follow-up is limited. In addition, fingerprint cards are not being sent to DPS, and arrests that have not been entered into APSIN create other backlogs of unknown size.

All authorized users of APSIN can tap the existing criminal history repository. Agencies use this information for general inquiry, making bail setting decisions, and developing pre-sentence reports. Users seem pleased with the inquiry capabilities of APSIN, although many would prefer a different format for the printout.

DPS has been working with interagency committees to set standards for both the reporting and processing of information, and the data elements stored in the repository. Standards for data elements such as defendant's name, date of birth, social security number, the arrest tracking number, and a common person identifier have been adopted or considered. As the number of data elements in the repository increases and as DPS regulates new information for the repository, more standards will be needed.

2. Overview of Existing Technology at DPS.

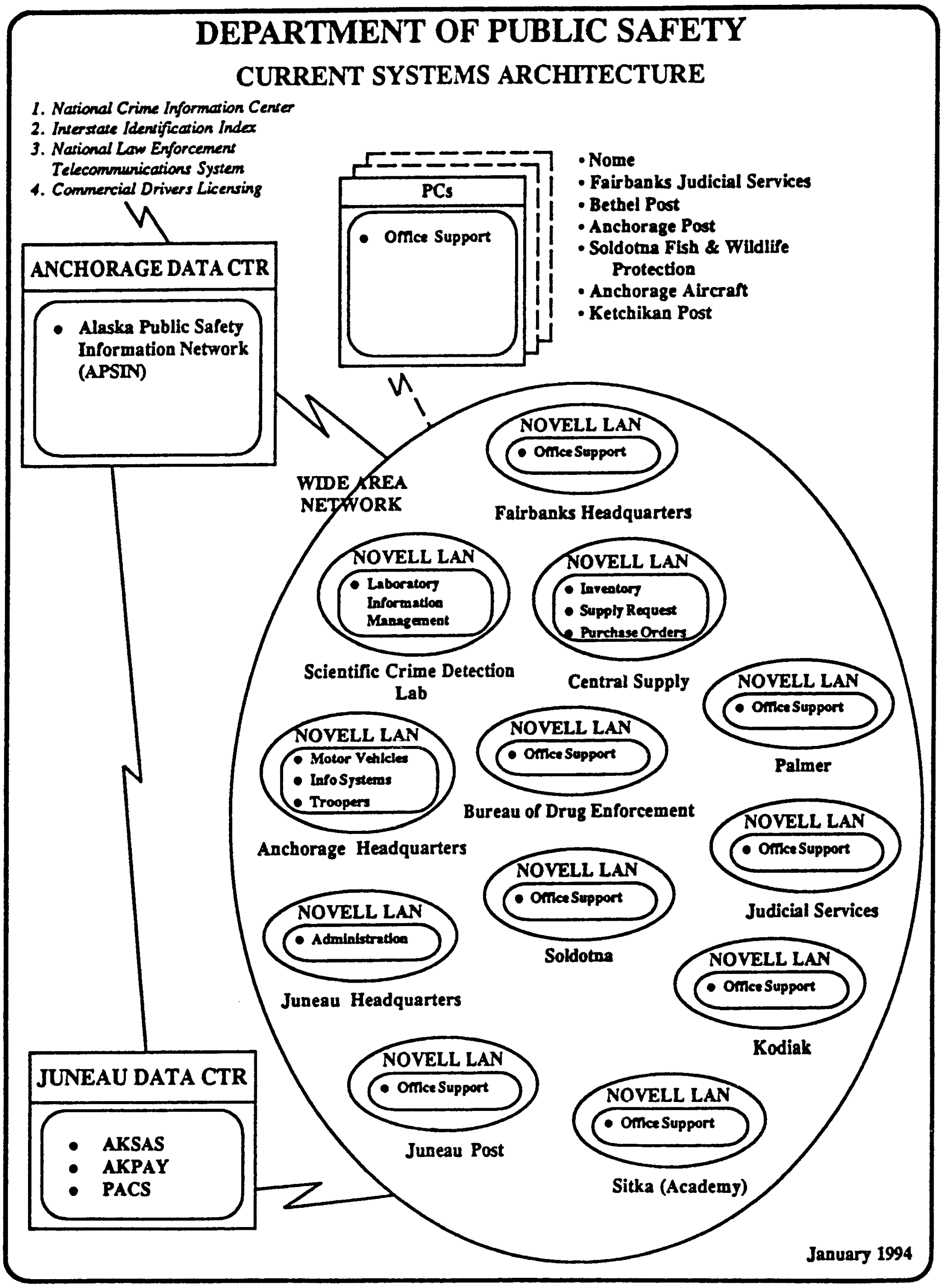
DPS uses a variety of hardware, including the state mainframe, file servers, and personal computers.[15] It uses mainframe, client/server and PC software. Its major mainframe application software is the Alaska Public Safety Information Network (APSIN).[16] DPS uses both mainframe (SNA) and LAN/WAN communications networks. In addition, DPS is developing a new Trooper Case Management System (CRIMES) which uses client/server technology.

[15] Figure 8 shows the DPS system architecture.

[16] Other important mainframe applications include the Alaska Automated Fingerprint Identification System (AAFIS) and the Warrant Service Photograph File. Non-departmental applications systems processed through the state network include the National Law Enforcement Telecommunications System and the National Crime Information Center (NCIC). These applications are discussed in greater detail below.

FIGURE 8

INFORMATION SYSTEMS DIAGRAMS



a. Current Hardware Environment at DPS.

DPS uses a mixture of mainframes, file servers, and personal computers. The processors are accessed using a variety of PC's, non-intelligent terminals, and printers. Equipment available at some of the sixty-seven DPS facilities throughout the state includes 358 personal computers,[17] 116 mainframe terminals,[18] and 409 printers.[19]

Numerous devices, located in both state and local agencies, are connected directly or indirectly into the AMDAHL. Approximately 787 of the connected devices--including terminals, PC's, and printers--access the DPS applications. Connections exist through the state telecommunications network to the state's mainframe at the Juneau Data Center (JDC), providing DPS users with access to additional state applications.

DPS has established hardware acquisition standards for the WAN, LAN's, and PC's at departmental and divisional levels. Standards ensure compatibility, and facilitate support and training.

b. Current Communications Environment at DPS

DPS currently communicates using both mainframe connections and local- and wide-area networks. Both mainframe and WAN communications for DPS's system use the DIS's communications network.

[17] Almost all are Compaq PC's of various models, the DPS standard. The few exceptions are IBM PC's. A small number are Compaq Laptop models. All are DOS compatible. Not included in this count are a small number of Macintosh computers acquired for special projects. No Macintosh computers are connected to the network.

[18] These are Telex or IBM non-intelligent terminals.

[19] These consist of a mixture of various models of Hewlett Packard LaserJet and NEC dot matrix printers.

1. **Mainframe communications.** SNA leased-line circuits are currently in place between each DPS facility connected into the state network and one of three communications hubs: Juneau, Anchorage, or Fairbanks.[20]

2. **LAN/WAN communications.** Thirteen existing LAN's[21] at five DPS facilities enable DPS users to share computer resources more effectively by distributing data bases and processing loads and facilitating sharing of peripherals, software, and files. DPS uses the WAN to transmit electronic mail (E-mail) and transfer data files. The DPS WAN segments connect into the state's WAN network, with DOA hubs located in Anchorage, Juneau, and Fairbanks.[22]

   In addition to the WAN network, Rabbit gateways provide access for some of the LAN devices into the front-end processors (FEP) of the SNA network. Thus, DPS can communicate through either the WAN or SNA networks.

c. *Current Mainframe Software Environment*

A number of applications administered by DPS reside on the DIS mainframe. In addition, DPS personnel access a number of external information systems through the state network. This section provides brief descriptions of these systems.

[20] The Juneau-Anchorage link, requiring double satellite hops, has recently been upgraded to a terrestrial microwave link in order to improve the five-kilobits-per-second (KPS) throughput rate. T1 connections between Juneau and Anchorage and Anchorage and Fairbanks are also established. Circuits into the hubs vary from 4.8 to 19.2 KPS. In-town access into each hub is typically 9.6 KPS, with some multi-drop lines.

[21] The LAN's are connected into token ring WAN segments. The two LAN's in Juneau form one segment.

[22] The DPS LAN/WAN network uses the following standard software: Novell Netware, Version 3.11; Network Schedule, Version 1.5; Da Vinci Electronic Mail, Version 2.0; Da Vinci Name Services; and Novell Mail Handler System (MHS). The standard topology is token ring. As with the SNA network, T1 leased-line circuits connect the WAN hubs. Cisco AGS+ routers are attached to the WAN hubs and the two DPS LAN servers are connected to the WAN hubs.

1. **Mainframe Systems Software Environment** DPS currently uses a variety of mainframe systems software.[23]

2. **Mainframe Applications Software Environment**

APSIN

The Alaska Public Safety Information Network (APSIN) is DPS' major application.[24] DPS uses APSIN for much of its data processing, including functions related to providing statewide criminal history data, vehicle registration, driver licensing, case management, and administrative data. Approximately 2,050 users access the system, which contains about 22 million records.

APSIN was developed around a master person index, meaning that each individual has a unique identifier referred to as the ID/LIC number. The identifier used is the Alaska driver license number, if one has been issued. Alternatively, it may be the state of Alaska photo identification card number. Non-residents may also be entered into the master person file using an individual identification number. These person records can be accessed by ID/LIC number, social security number, name, soundex of name, gender, race, and date of birth.

APSIN is composed of five criminal history modules: APSIN Criminal History,[25] APSIN Full Criminal History,[26] APSIN Secondary Criminal

[23] The mainframe software used by DPS includes CICS, ADABAS, NATURAL, NATURAL CONNECTION, SUPERNATURAL, ADABAS NET-WORK, PREDICT, and COBOL II.

[24] Residing on the AMDAHL in Anchorage, APSIN uses the ADABAS data base management system and consists of approximately 1,400 programs coded primarily in NATURAL, as well as some using command-level CICS and COBOL II. Connected devices include 787 terminals, PC's, and printers.

[25] The APSIN Criminal History provides arrest, conviction, and personal description data for adults with criminal history. This information is selected and formatted to meet dissemination criteria.

[26] The APSIN Full Criminal History provides arrest, conviction, and personal descriptors, including arrests without convictions and without final disposition data. Fewer users are authorized to access this module than the Criminal History module.

History,[27] APSIN Fish & Wildlife Criminal History,[28] and APSIN Warrants.[29] Generally, each module contains different data and serves a different user community.

AAFIS

DPS has other mainframe applications and files that are not part of APSIN. These include the Alaska Automated Fingerprint Identification System (AAFIS), the Warrant Service Photograph File,[30] and the Duplicate DMV Photograph File.[31]

AAFIS has been in place for twelve years and represents technology that is at least fifteen years old. It is an NEC system that positively identifies individuals through comparison of ten-print cards and latent fingerprints to digitized fingerprints stored in the system. The ID/LIC number serves as the cross-reference between APSIN and AAFIS. The presence of fingerprint records is flagged in the master person record on APSIN.

Alaska's AFIS system is incapable of supporting the transaction volumes, speeds, and data base capacity of the state's current and future identification needs. DPS currently spends $175,000 per year just to maintain this older system, and these costs will increase in the

[27] The APSIN Secondary Criminal History is the most limited criminal history module. Users authorized for this module are not law enforcement personnel. This module provides only conviction information, displaying no arrest-without-conviction data.

[28] The APSIN Fish & Wildlife Criminal History provides criminal history data related specifically to fish and wildlife violations.

[29] APSIN Warrants provides the centralized tracking of outstanding want and warrant information for all criminal justice agencies in Alaska. Missing persons also are included in this file, with a status of "locate."

[30] The Warrant Service Photograph File is a manual file of mugshot photographs maintained to facilitate servicing of warrants.

[31] The Duplicate DMV Photograph File is a manual file of duplicate driver license photographs used for photo lineups.

future. These maintenance costs, coupled with upgrades that will be necessary to make the system work, will far exceed the cost of replacing it with a new system, and still will not provide functionality.

Non-Departmental Applications

DPS personnel access six non-departmental applications through the state network. These non-departmental applications include the National Law Enforcement Telecommunications System (NLETS), the National Crime Information Center (NCIC), the Western Identification Network (WIN), the Canadian Police Information Center (CPIC), the Commercial Driver's License (CDL), and the Problem Driver Pointer System. Each of these systems is explained below.

DPS has a direct link between NLETS and APSIN. DPS controls state and local agencies' access to NLETS. Authorized users may access these files. APSIN processes criminal justice inquiries from NLETS users outside the state of Alaska. APSIN also has a direct connection to NCIC, which allows DPS to control the access by other agencies in Alaska. Many of the inquiries into NCIC are triggered by inquiries into APSIN.

DPS provides access to the Western Identification Network. This network gives access to data contained on NEC AFIS systems, including Alaska's, in the western United States.

DPS provides access to the Canadian Police Information Center, a Canadian system, through NLETS. Standard NLETS inquiry transactions are supported.

The Commercial Driver's License application provides access to national commercial driver's licensing data. The Problem Driver Pointer System (PDPS) provides access to national data on problem drivers.

d. Current LAN/WAN Software Environment

Software currently running on the LAN/WAN includes Novell Netware, Network Scheduler, and MS-DOS.[32] Applications currently residing on the LAN/WAN's include word processing,[33] electronic mail,[34] and access into the state of Alaska network to other state applications.

e. Current DOS PC Software Environment

DPS has 358 personal computers.[35] DPS has word processing,[36] spreadsheet,[37] and data base management system[38] packages for its PCs.

f. Client/Server Hardware/Software Suite of Products

DPS has acquired its client/server equipment in connection with the CRIMES project. DPS has a Unix machine,[39] and the data base software[40] and tools needed to develop the CRIMES program.[41]

[32] The Da Vinci Electronic Mail System and Novell Netware provide security.

[33] Case narratives, budget forms for all divisions, memos, letters, and other department documents are processed in WordPerfect.

[34] Da Vinci Electronic Mail within LAN's, and Novell MHS, manage transmissions between Juneau and Anchorage through the WAN hubs.

[35] These Compaq and IBM computers run MS-DOS and Windows 3.1.

[36] DPS uses WordPerfect.

[37] DPS uses LOTUS and EXCEL.

[38] DPS uses Rbase. In addition, a number of small applications addressing specific information requirements were developed in Rbase, Foxpro, WordPerfect, or spreadsheet packages.

[39] The Unix box is an IBM RS/6000 Unix (AIX).

[40] DPS uses the Oracle data base.

[41] The other products selected for this project include: development software (Microsoft ACCESS, ACCESS Distribution kit, and Visual Basic Professional Edition); ASPIN Access Software (ADADDE, NET-WORK for Windows, NET-WORK for MVS, NET-WORK for OS/2, OS/2 2.0, OS/2 Extended Services); a low-level language compiler (Microsoft Visual C++; TCP/IP Software Development Kit--SPRY Air

3. Future Technology Development Plans.

DPS published an Information Systems Management Plan in August, 1993. The plan details tactical projects for the department to work on during the next thirty-six months. The plan recommends that DPS move as many new and current programs to client/server hardware and software as possible while still using the mainframe for large data bases. The plan predicts a funding shortfall of $4,256,000 over the next three years for the tactical projects described.

Under the plan, new programs, such as CRIMES, vehicle search, and application tracking will use distributed data processing strategies that will be integrated into the existing network. Anticipated hardware changes include the eventual replacement of all 116 Telex and IBM terminals with DOS-compatible PC's.[42] Replacement of DMV terminals has received the highest priority.

Efforts also are underway to acquire additional file servers.[43] Once the CRIMES system is running, the department intends to move other APSIN applications from the mainframe to this or a similar suite of client server hardware and software tools. We believe the general direction detailed in this plan is reasonable and the current efforts to pursue client server technologies for the new CRIMES application makes sense.[44]

Finally, the department's future technology needs will be affected by a bill submitted during the 1994 legislative session. This bill mandates fingerprinting for all offenses and includes fingerprints in the central criminal history repository to ensure positive offender identification; it also requires each criminal justice agency to submit

Services); word processing software (Microsoft Word for Windows); a client workstation GUI environment (Microsoft Windows 3.1); a client workstation operating system (DOS 5.0); and a decision support data base (Oracle).

[42] These PC's will have 3270-emulation capabilities. Minimum standards provide for 386 machines with hard drives, tape backups, and surge protectors.

[43] New file servers have been specified as DOS-compatible 486/50 megahertz machines with 340-megabyte disk drives, tape drive backup devices, and uninterruptable power supplies.

[44] We recommend that the department also enlarge the data base for the criminal history repository to include the new data elements needed to track charges accurately, the event-reporting elements that will be required by the pending APSIN legislation, and the key components of the eighteen SEARCH elements. See Chapter VI for details.

"reportable events" information about case processing to the central criminal history repository. The bill provides that the Commissioner of DPS will promulgate regulations for data timeliness, accuracy and completeness, as well as agency reporting. While this bill is crucial to improving Alaska's criminal history records, the current AFFIS system will not be able to handle the workload increase created by the mandatory fingerprinting requirements.

D. Department of Law

1. Information Needs and Resources of DOL.

The Criminal Division of the Department of Law (DOL) manages its criminal caseload using the Prosecutor's Case Management Information System (PROMIS).[45] This system, which has operated since 1982, runs on the state mainframe. DOL has six staff members (five data clerks and a supervisor) who enter information from the Criminal Case Intake and Disposition form into PROMIS;[46] however, the department has no in-house analyst/programmer. Thus, PROMIS currently is supported by an independent contractor.[47]

While it is adequate for the storage and retrieval of basic case information, PROMIS does not meet DOL's other data processing needs. Because of its age, the PROMIS system requires continued maintenance. Other problems involve limits on the number of records,[48] inability to do scheduling well, and inability to provide statistics in a useful form. In addition, PROMIS does not meet the needs of the smaller offices.

[45] The DOL has a total of eight major statewide software applications: Attorney Work Management, Attorney Timekeeping, Criminal Case Management, Litigation Support, Work Product Index, Legal Opinion Index, Brief Bank, and PROMIS. All these systems reside on the Juneau Data Center mainframe computer. Figure 9 shows the DOL's current system architecture.

[46] DOL has a personnel budget of $250,000 for these staff members.

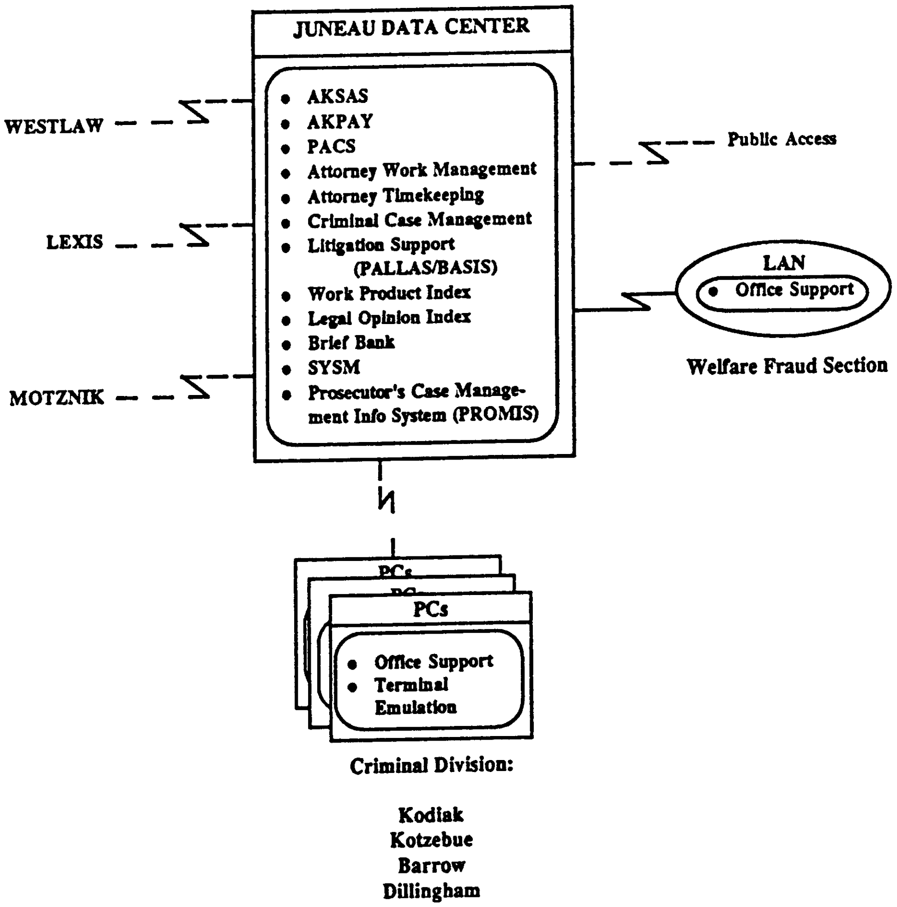
[47] The PROMIS source code is maintained by an independent contractor; this maintenance contract costs DOL $25,000 per year.

[48] PROMIS data undergoes periodic purges because it exceeds its internal limit of one million records.

FIGURE 9

INFORMATION SYSTEMS DIAGRAMS

DEPARTMENT OF LAW
CURRENT SYSTEMS ARCHITECTURE



September 1992

Alaska 1994 Information Management Plan

Appendix F.17

DRAFT

19/5/2SYSTEMS.PM5/17—2/94

Nor does PROMIS meet the information-sharing needs of the other criminal justice agencies. PROMIS cannot easily be modified to permit integrating information with other systems. For example, DPS currently is attempting to retrieve from PROMIS the "declines to prosecute" and to post them to the CCH. Matching these records to the corresponding CCH entry is proving difficult. Moreover, adding new data elements is difficult and expensive, further supporting the need to replace PROMIS.

DOL would like to replace PROMIS with a more flexible application that requires less maintenance and meets DOL's information needs more comprehensively. In addition, DOL acknowledges the importance of a system that will permit it to share information with the other criminal justice agencies, in particular, with the DPS criminal history repository.

2. Overview of Existing Technology at DOL.

DOL has eight separate mainframe software applications to support its data processing needs statewide, including the PROMIS system. All applications run on the Juneau Data Center.

a. *Software Applications*

The PROMIS system is written in COBOL. It has a unique, proprietary file structure and employs old technologies.[49]

b. *Hardware*

The DOL application software resides on a mainframe in Juneau. These systems use only a small portion of the hardware capacity; they are accessible through the DIS backbone network.

[49] The file structure does not conform to the VSAM standard.

3. *Future Technology Development Plans.*

The Department of Law should replace PROMIS. PROMIS does not meet DOL's internal information management needs, nor does it lend itself to sharing information with other criminal justice agencies.

DOL should first analyze its business needs and purchase a package that will meet those needs. If no such package is available, then DOL should develop a new system, with the possible support of the DPS Information Systems Section.[50] Whether DOL builds or buys a new case management system, that new system should be consistent with the technology alternative recommended in this report.

The new case management system should take advantage of the newer technologies and meet DOL's needs as determined by its business re-engineering analysis. While analyzing its information needs, DOL should not overlook the need to share information with the other criminal justice agencies, particularly with the DPS criminal history repository.[51] In addition, the new system should address victim notification reporting requirements as mandated by law.[52]

E. Department of Corrections.

1. *Information Needs and Resources of DOC.*

The Department of Corrections (DOC) maintains a statewide tracking system (OBSCIS), an inmate accounting program (HOFA), a probation caseload register/workload statistics program and a Roscoe batch-reporting system (R-BRS). These systems all operate on the state's mainframe in Anchorage and are accessed by the thirteen correctional centers, three pretrial facilities, thirteen district probation offices,

[50] Because the DOL has no internal technical staff, it could not build or buy a new system without assistance from another agency or from independent contractors. DOL has expressed a willingness to work closely with DPS, even to the extent of developing a joint system to be developed and supported by the DPS technical staff.

[51] Modifying the current PROMIS system to accommodate new data elements is impractical. Although the agencies have agreed on standards for key data elements such as the person identifier and the ATN, these elements must be placed in "open" fields that are not required or edited by the system.

[52] *See* Alaska Statutes 12.61.015.

and three administrative offices through the state's SNA backbone network.[53] In addition to its offender tracking and inmate accounting responsibilities, DOC fingerprints most offenders at its booking stations. Fingerprinting is crucial to the positive identification component of a criminal history repository.

DOC's current systems do not meet the department's information needs and must be replaced. A management audit by KPMC Peat Marwick in 1991 concluded that "the OBSCIS and HOFA systems are not relied upon, used, nor understood by department staff." Peat Marwick found that the systems lack real capabilities, and also that staff lack training to use the systems. Our 1994 interviews indicated that many of these same problems still exist, despite enhancements made to OBSCIS since 1991.

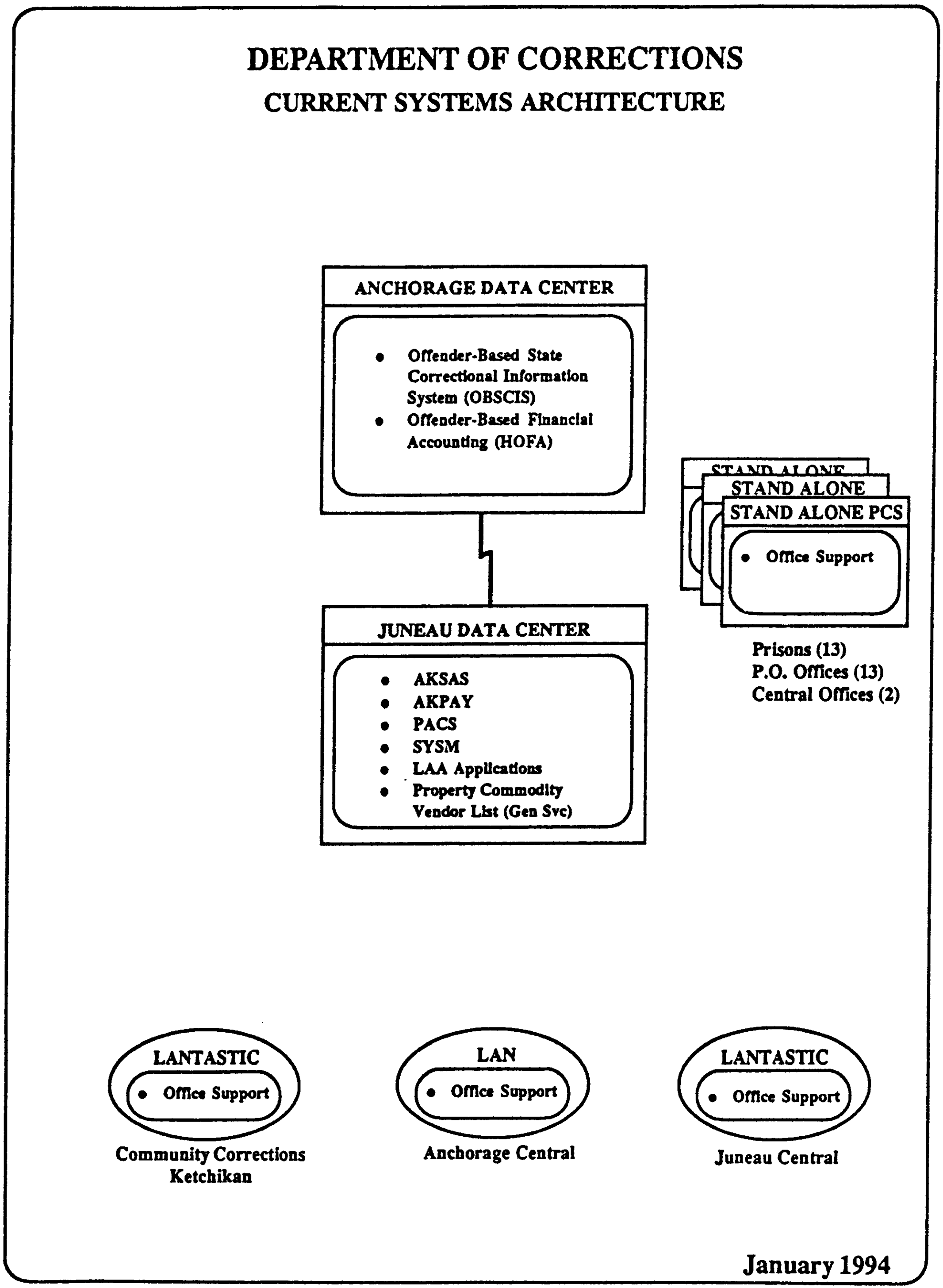
OBSCIS cannot share information with other criminal justice agencies. The two main constraints to sharing information are the incompatibility of DOC's old technology with other criminal justice systems, and the difficulty of modifying DOC's systems. Incorporating new data element standards into OBSCIS is very difficult. Thus, although the DOC has participated in the development of standards and recognizes the importance of sharing information, OBSCIS prevents it from implementing some agreed-upon standards and from providing needed data to other agencies. Second, DOC systems technology does not use a data base facility and is cumbersome to access. Third, the quality of the data in the systems is questionable and therefore agencies cannot rely on it.[54]

[53] The DOC's current system architecture is described in Figure 10.

[54] Nonetheless, a number of agencies draw information for limited purposes from OBSCIS. (These agencies include DPS, local police departments, the PDA, the Department of Revenue Permanent Fund and Child Support Divisions, the Court System, Health and Social Services, the Judicial Council, DOL, and the U.S. Probation Office.)

FIGURE 10

INFORMATION SYSTEMS DIAGRAMS



DEPARTMENT OF CORRECTIONS
CURRENT SYSTEMS ARCHITECTURE

January 1994

Appendix F.10

Alaska 1994 Information Management Plan

DRAFT

2/94—19/5/2SYSTEMS.PM5/10

DOC has a small data processing unit consisting of one data processing manager and two analyst/programmers.[55] This staffing is insufficient even to maintain the current system. Staff have requested numerous time-consuming enhancements to OBSCIS, leaving little time for planning or new system design. In addition, the current staff has no experience with the new hardware and data base technologies that will be necessary to any redesign effort.

2. Overview of Existing Technology at DOC.

DOC uses three mainframe software applications installed in the early 1980's. Most of its applications use 1960's network technology and equipment. Much of DOC's hardware (printers, controllers, terminals, and modems) is too old to use the newer technologies.

a. Software Applications

The department's OBSCIS system, HOFA program and probation caseload register/workload statistics program are COBOL II/CICS programs running on the Department of Administration's mainframe computer in Anchorage. Since their initial installation in the early 1980's, these applications have been maintained, remodeled, and added to by several generations of programming staff. OBSCIS is a menu-driven application, using 1960's data processing methods and design.[56] Files and data elements are accessible to other applications in a batch-only mode.

The booking office uses the National Crime Information Center (NCIC) and National Law Enforcement Telecommunications System (NLETS), available through APSIN, to add missing demographic information and search for outstanding warrants or other criminal history information at admission. This information is obtained on line.

[55] DOC spends approximately $400,000 per year for its data staff and the rate-based charges from DIA for mainframe use.

[56] OBSCIS runs in the Department of Public Safety's CICS region and uses VSAM files.

b. Hardware

The DOC and other agencies access OBSCIS and HOFA applications through the state's SNA network. OBSCIS and HOFA provides 24-hour-a-day tracking and accounting functions for correctional facilities and probation offices. Many of the department's modems, controllers, printers, and terminals were obtained from other state agencies, state surplus, or were purchased in the early to mid 1980's. This equipment must be replaced because it is too old to use with the newer technologies.

c. Telecommunications

As a part of the state's SNA network, the department has access to the state's E-mail system, SYSM. SYSM permits written mail, notes, and files to be passed to any user's account on the network. People who have access to APSIN can communicate through the Administrative Messages facility.

In addition to the state's SNA network, the department has three local area networks. These LAN's are located in Ketchikan, Juneau, and Anchorage.[57]

3. Future Technology Development Plans.

Like DOL, DOC is a prime candidate for replacement of its principal systems. Also like DOL, DOC can take advantage of the newer technologies that will permit better compatibility, reliability, and user friendliness. The department should use the same business re-engineering method suggested for DOL to assess its internal information needs as well as the information-sharing needs of the other criminal justice agencies.

DOC should include in its re-engineering analysis the requirement that fingerprints be taken in every case and that the quality of the prints be adequate for

[57] These peer-to-peer LAN's provide peripheral sharing and gateway/3270 emulation in their respective locations.

positive identification.[58] The agency's new information system also should permit it to transfer into the criminal history repository information about parole and probation status, status of the offender (i.e., released or where incarcerated), and revocations and escapes. The system also must account for DOC's need to get information about the time offenders serve i contract jails or other facilities not maintained by DOC.

DOC is moving toward local area networks (LAN's) in a client/server environment using microcomputers as intelligent workstations. These LAN's/ microcomputers will provide both word processing and 3270 emulation capability for the department's current and future needs.

F. Alaska Court System

1. *Information Needs and Resources of the Alaska Court System.*

The Alaska Court System is a significant provider and user of criminal history information. It operates two major systems: a records system for the Court of Appeals and the Supreme Court, and a trial court system.[59] Both were developed and are maintained by the Technical Operations section.[60] Both presently are being redesigned and redeveloped.

While the court system did not use a formal tactical and strategic planning process to redesign its systems, it devoted much thought and user input to the redesigns. For example, the statewide trial court information system (CIPS) general design was developed by a users committee working with an analyst over the course of three years. The appellate court information system was developed by a separate users committee during the past year. The court system contracted with an independent contractor to

[58] The proposed legislation mandating fingerprinting for felony cases and, eventually, misdemeanor cases will affect the workload of DOC staff. DOC staff workload also will be affected as regulations are promulgated that require criminal history repository data.

[59] The ACS also has several administrative applications, such as service and equipment inventory, microfilming, and storage and supply. These are supported by the in-house technical data staff.

[60] Technical Operations consists of five analyst/programmers, four electronic technicians, a supervisor, and clerical staff. This section supports the court applications at twenty-eight trial court and appellate court sites.

develop the trial court system modules.[61] All modules are to be delivered by the spring of 1995, with implementation to begin soon thereafter. The appellate design will be developed and implemented when funding for contract services becomes available, or when internal staff become available to work on the system.

The existing court case management system does not track dispositions at the charge/count level, does not contain the date of disposition, does not produce an electronic judgment form, and does not transfer this information electronically to any of the other criminal justice agencies. However, the new case management system will track case progress at the charge/count level (including disposition for each count), will provide the date of disposition, and will generate an electronic judgment form. The court system has agreed to provide any of this information to criminal justice agencies and the criminal history repository in electronic form.[62]

The court system has cooperated with criminal justice agencies' efforts, through the Technical Users' Group and the inter-agency Computer Policy Group, to standardize data elements and to provide electronic data to other agencies when the exact requirements have been defined. For example, the court system helped establish standards for date of birth, social security number, court case number, person identifier, ATN, statutes, and names. It has agreed to use these standards where possible or to format data to be transmitted to other agencies in accordance with the standards. In addition, it has incorporated these standards, where possible, into its new system design.

The court system plays a pivotal role in providing information to the criminal history repository. Of particular importance is the submittal of judgments for disposition reporting. The court system uses the criminal history information at the time of bail setting and at sentencing.

[61] The general design includes the following modules: civil cases, probate, exhibits, motions, judge assignment, numbers assignment, warrants, traffic cases, criminal cases, childrens' matters, accounting, in-court calendaring, jury management, forms and ad hoc reporting.

[62] A number of criminal justice users expressed interest in querying the court criminal case data. The court seems willing to permit this access, recognizing, however, that the court's twenty-eight trial court sites are not linked by a network. The sites currently communicate electronically by way of Unix UUCP, which allows file transfer between sites by way of voice grade lines at 19.2 baud.

2. Overview of Existing Technology at the Court System.

The court system runs most of its software on its own series of client/server devices but does use the state mainframe to operate the Jury Selection system, to access the state's accounting and personnel/payroll systems, and to access APSIN for traffic citations, criminal records, and warrant information. The court system uses Unix and relational data base technologies for its operational systems.

a. Software Applications

In addition to its jury system and the access to the other state systems on the mainframe, the court system operates a number of systems on its own in-house hardware. Two major systems, currently being redesigned, are the Appellate Court System and the Trial Court System.

The Appellate Court System implemented in 1984 consists of sixty BASIC programs using the ISAM file structure. Twelve terminals connect to this stand-alone system.[63] All personnel in the clerk's office, as well as central staff and judicial chambers, have access to a Unix-based system supporting WordPerfect word processing, E-mail and document transfer and providing public on-line access to various appellate court documents (new opinions, etc.). Several small Progress relational data bases have been installed on this system for the use of the judges' secretaries. Approximately fifty terminals (a mixture of dumb terminals and PC's) connect to this system.

The trial court system operates under Unix and currently runs approximately 200 UXBASIC programs using ISAM file structures. These sites, installed between 1982 and 1988, have undergone several significant revisions. In the last year, the court system added ten "small court" sites which operate with a single PC acting as a host for two to three dumb terminals. These PC sites also are operating under Unix. All sites support WordPerfect for word processing, statewide E-mail and document transfer (via UUCP) and remote access (dial-up). Twenty-eight court sites currently have operational systems, using the same software and file structures at each site. The court system also has a number of administrative systems (service and equipment inventory, microfilming,

[63] The appellate clerks in Fairbanks and Juneau have remote access to the system.

storage and supply, administrative packages, etc.). All of these systems operate under Unix and most have been converted to Progress data bases.

b. Hardware

Overall, the court system currently supports about 600 users with a variety of hardware. Eighteen sites use AT&T StarServer E computers.[64] The largest system, in the Anchorage Trial court, supports 175 terminals and about fifty printers.[65] All of the AT&T systems can communicate with other state systems (such as DPS's APSIN) via the state telecommunications network.[66]

The PC-based sites use Everex 486 PC's running Unix. An intelligent port-sharing card enables them to support peripherals (two to three dumb terminals, printers, etc.) through an intelligent port-sharing card.[67]

In addition to these host systems, the court system maintains approximately 155 PC's (140 desktop and fifteen laptop).[68] All PC's use a terminal emulator file transfer package to access their local Unix systems.[69] The package allows them to be a terminal on the host system or to make use of the host system for document storage, E-mail, etc.

The court system does not plan to change its hardware as part of its system redesign. With the support of the technical operations staff, the court system plans to use its existing equipment.

[64] These are 486-based multi-processors. The standard configuration is one processor, 16MB of RAM, 600 MB of hard disk storage, and thirty-two ports. These systems can expand to four 486 processors, 256MB of RAM, 14GB of hard disk storage and 512 ports.

[65] This particular system uses three processors, 64MB of RAM, 2.5 GB of hard disk storage and has 256 ports.

[66] All systems have SNA/SDLC cards installed.

[67] The court system has a total of twelve Everex 486 PC Units, twenty AT&T StarServer E Units and 620 Dumb Terminals. They have 16MB RAM and 300 MB hard disk storage.

[68] In addition, the court system has 187 laser printers and sixty-eight impact Printers.

[69] This package is called Rapport.

c. Telecommunications

The court system currently does not operate any LAN's or WAN's. Instead, it communicates between its thirty-two sites/systems using the Unix UUCP communications capability. This arrangement allows the court system to provide its users menu-driven, statewide E-mail and file transfer between sites. Communications use voice-grade telephone lines and Telebit modems.[70] These same procedures could be used to allow users real-time access to other remote court systems, but the court system has not implemented this option. The StarServer E computers are all equipped with SNA/SDLC firmware and software. These courts can function as remote controllers on the state network to access APSIN and to access/update the Division of Motor Vehicles' records.

3. Future Technology Development Plans.

The court system's new criminal case management system will track charges, counts and final disposition reporting information important to the criminal history repository and to other criminal justice agencies. While waiting for its new system to be implemented, however, the court system could begin designing interfaces for electronic data transfer to the criminal history repository. This design plan should address the formatting of data, the frequency of transfer, the method by which data will be pulled into a central facility, and whether inquiry into or the transfer of data to the court system is practical. Because the court system has tried to incorporate common data standards into its new system, matching records electronically to records in the CCH repository will be fairly easy.

G. Department of Health and Social Services, Division of Family & Youth Services

1. Information Needs and Resources of DFYS.

The mission of the Division of Family & Youth Services (DFYS) is to protect children and vulnerable adults at risk of abuse and neglect and to rehabilitate youthful offenders while providing community protection. The agency is organized into three

[70] This arrangement allows the sites to communicate at 19.2 KPS, which is adequate for their current purposes.

regions and has thirty-six Family Services offices, three Juvenile Probation offices and operates five youth facilities. The central administrative office is located in Juneau.

DFYS needs criminal history repository information to conduct background checks on potential foster parents, other child care providers, and its youth corrections staff. It also uses criminal history information to conduct recidivism research. This information is accessed through the State's SNA backbone network; however, DFYS has found that the available criminal history information is not complete. For example, on occasion no criminal records have been found for a foster parent applicant who later is discovered to have had a criminal record.

DFYS does not directly contribute information to the criminal history repository. It fingerprints adjudicated juveniles remanded to McLaughlin and forwards the information to DPS for entry in AFIS. DFYS makes records of adjudicated juveniles available to DOC for presentence reporting.

2. *Overview of Existing Technology at DFYS.*

DFYS has two information systems, one running on the state mainframe and another running on PC's. Mainframe applications are used to manage licensed child care facilities, pay care providers such as foster homes, and manage client data for the payment function. The client data on the mainframe duplicates data on the primary client system. The primary client information system database (PROBER) runs on PC's and includes client classification, case management, workload accounting, and management information. This system functions as the youthful offender history repository and includes information on charging, disposition, classification, probation, and institutional placement. Each DFYS office maintains a complete or partial database and updates it daily in an exchange process with the central database in Juneau. The exchange takes place over telephone lines and the DH&SS WAN to LAN sites. DFYS has LAN's operating at six locations.

3. *Future Technology Development Plans.*

DFYS is in the process of porting the mainframe based facilities management information system to its PC based application. DFYS also is conducting a feasibility study to develop a similar replacement for the payment system. The objective is to integrate all DFYS information systems on the same platform. The PROBER database currently is being rewritten as a client/server application with multi-user capability, expanded field capacity and improved transaction processing. The enhancements are expected to be operational in the summer of 1994. DFYS also has requested both state and federal funding to redevelop its entire information system using newer database technologies to meet new federal reporting requirements, automate more processes and produce decision support for line workers. The placement system will require interfaces with EIS and the Child Support system. Interface with the criminal history repository also will be addressed.

DPS has asked DFYS to make available offender information from the client database so that DPS can retrieve information about arrested and adjudicated juveniles. During systems redesign, DFYS will explore electronic interface for this information exchange. In the future, DFYS would like access to OBSCIS data for the purpose of conducting recidivism research to determine how often juvenile offenders enter the adult system.

H. Public Defender Agency

1. Information Needs and Resources of the Public Defender.

The Public Defender Agency (PDA) has eleven offices statewide with fifty-four attorneys, ten investigators, and approximately twenty-two secretaries supporting both civil and criminal caseloads. The PDA principally uses information from other criminal justice agencies. Its investigators have access to APSIN to retrieve updated CCH information, driver's license and witness information. Agency staff use a terminal at the court system in Anchorage to retrieve court records and get access to APSIN. The PDA is concerned, however, that the level of access permitted by the original AJIS statute[71] to APSIN data would continue under the proposed new APSIN legislation.

The PDA has no internal technical staff. It has relied on an independent computer services firm, Helleck & Associates, for support.

[71] ALASKA STATUTES 12.62.

2. Overview of Existing Technology at the Public Defender.

Despite historically inadequate funding, the agency has, over the last year and a half, been acquiring hardware and software, establishing networks, and using an independent software consultant to develop a new case management system.

a. Software.

An independent consultant recently completed a case management system in Foxpro. Implementation has begun in Anchorage. The system, which includes all felony, misdemeanor, and appeals cases, should be operating statewide by summer.

The agency's PCs run WordPerfect, except for Fairbanks, which runs Microsoft Word. The agency also has set up WestLaw access in most offices and is establishing a brief bank in Anchorage that eventually will be available statewide through modem access.

b. Hardware

After a final purchase of computer equipment in February, 1994, the agency has placed a computer on almost everyone's desk. Each office now has at least 386sx PC's, except Fairbanks which uses Apple Macintosh computers.

c. Communications

A Novell network is up and running in Anchorage. An Apple Talk network has been installed in Fairbanks. Kenai has used an old Lantastic network. The other offices will have printer-sharing devices. Barrow and Palmer are testing these devices. The other offices will install them as soon as possible. The agency has purchased the software for an E-mail system, but has not had the time to get it running.

3. Future Technology Development Plans.

Limited funding renders future growth in technology unlikely. The PDA can improve its ability to give and receive criminal justice information. For example, the PDA will act as a clearinghouse for other defense attorneys needing criminal justice information if the district attorney's office finds that responsibility to be too burdensome.[72] The agency will "sanitize" its case management system information, omitting children's cases and other confidential material, and making the resulting case information available to other criminal justice agencies. For example, the PDA could provide a list of people it represents in criminal matters.

The PDA supports the SEARCH recommendations about a new format for the rap sheet and the use of common identifiers. The PDA has network access into APSIN and the criminal history repository limited to one PC for security reasons. It also has access to OBSCIS to locate prisoners within the correctional system.

Technical issues constraining electronic data sharing include connectivity and compatibility. First, the agency needs network access to other criminal justice agency systems. Second, the Fairbanks office's use of Macintosh computers presents a problem. Finally, the PDA staff will need extensive training on its new in-house system and on using other agency systems.

I. Anchorage Police Department (APD)

1. Information Needs and Resources of the APD.

Residents of the Municipality of Anchorage (MOA) comprise approximately one-half of the state's population. The APD serves approximately 200,000 of Anchorage's residents within its 203.2 square mile jurisdiction.[73]

After APD established a goal in 1980 to implement an integrated Computer-Aided Dispatching and Records Management system, MOA contracted in 1983 with Unisys to provide the system. APD began Phase I of implementing the police information system, PLIMS, in 1988, receiving and installing the remaining modules in 1989. Phase II began in 1990 with a two-year project to establish a police information network (APDI Net), and to integrate office automation with the APDI Net. During Phase II, completed in 1992, APD installed Macintosh computers and standard office automation functions, such

[72] An AJIS regulation, 6 AAC 60.060, envisioned this role for the PDA.

[73] This jurisdiction is divided into twelve patrol areas.

as word processing, spreadsheets, scheduling, and E-mail. Eight Unisys terminal emulation gateways integrate the PLIMS centralized crime information system into the network.

APD has found the PLIMS system less than satisfactory in the areas of data entry, retrieval, and format. The data entry process is cumbersome, requiring the use of too many screens. Retrieval of information is difficult because no executive on-line reporting module allows English-type ad hoc queries. In addition, employees find that screen layouts are difficult to read, and that the data are not organized consistently throughout the system.[74] Also, the system lacks automated statistical reporting features,[75] and lacks imaging capability.[76]

Other problems concern the lack of automated interfaces with other systems. There is no automated interface to APSIN or NCIC. Nor does Computer-Aided Dispatching (CAD) interface to the E911 system.[77] Third, there is no automated interface between PLIMS and the Macintosh systems where the interview tape transcriptions are entered. Fourth, the PLIMS Geobase and Municipal Public Works Geobase are separate, so that maintenance is duplicated on address, business and streets.

Yet more problems concern slow system response time. Batch reports and required system backups slow the system down. The PLIMS' system hardware is operating at capacity. Also, the CAD function consistently fails to meet its fast (one second or less) response time requirements.

The underlying and most important complaint is that the system lacks flexibility. Because PLIMS is a proprietary system owned by McGowan & Associates, McGowan has sole access to the source code and must develop all modifications and enhancements.

[74] For example, the same data field appears in different locations from screen to screen, even within the same logical module.

[75] APD personnel run existing reports and manually enter the data into their PCs for consolidation and formatting.

[76] Employees manually enter case and supplement information into PLIMS, if possible, and then store it in the manual archive files.

[77] Call takers must manually type into CAD the information that the E911 screen displays.

Thus, the system can not respond quickly enough to meet APD's rapidly changing business goals, and modifications come at a high cost to APD.

2. Overview of Existing Technology at APD.

APD runs its PLIMS system on a Unisys mainframe. In addition, it operates a Police Information Network which is integrated with office automation.

a. APD Mainframe Hardware

PLIMS runs on Unisys A6 and A1 mainframe computers. The A6 system is dedicated to running PLIMS. The A1 system is used to test new releases of PLIMS and to support PLIMS training activities, and as the back-up processor, should the A6 system fail.

The A6 Mainframe system is the primary system used to operate PLIMS. PLIMS was developed using LINC II, a fourth-generation language. While the A6 system operates the entire PLIMS network, the A1 system is expected to support only those sections that are deemed critical to the short-term operation of APD. Specifically, these include the Dispatch and Records sections. The PLIMS system hardware consists of processors,[78] shared devices,[79] terminals,[80] and printers.[81]

[78] A Unisys A6 single processor with 36 MB of memory and 840 MB of internal disk; a Unisys A1 single processor with 24 MB of memory and 1.12 GB of internal disk.

[79] Eight GB of M9710 disk, 1 GB of MD8 disk, (2) 2145 501P GCR tape steamers and (2) 650 LPM impact printers.

[80] Sixty Unisys T27 (capable of three sessions), (35) Unisys ET1100 (capable of two sessions).

[81] Twenty FACIT 4510, (19) Unisys AP310, (2) Unisys AP1350, (1) Unisys B9252, (1) Unisys AP1302, (1) Unisys AP1305, (1) Unisys AP1327, (2) Unisys AP1351, (2) Unisys AP1354, and (2) Unisys B9253.

b. APD APSIN/NCIC and DECnet Hardware

There are no external system interfaces at this time.[82] APD accesses APSIN and NCIC through the DPS SNA network using twenty-two Telex and 327X terminals.[83] APD accesses the Municipal DECnet through an SNA network of IBM terminals and TELEX terminals.[84]

c. APD Personal Computers

The Macintosh computer is APD's standard DeskTop workstation.[85] APD's personal computers use the Ethernet Network to access APDI Net.[86] The Ethernet backbone will be used for the implementation of future client/server systems and for the APD wide-area network.

Currently, four UNISYS PW workstations are networked to form the PAWN System Network. Diskettes of pawned articles are brought over to DPS weekly and loaded into APSIN to check against APSIN and NCIC files. This network will be upgraded with remote access in order to transfer PAWN information files to the state APSIN system.

Remote dial-in to APD is accomplished with a LanRover E/4 and two Shiva NetModem Es. All the dial-in lines operate at 9.6 KPS or less. Faster rates are unreliable with the Anchorage Telephone Utility analog phone lines.

[82] APD investigated developing an interface to APSIN and NCIC in 1989; however, it dropped that idea because the state required it to develop a statewide bisync interface for data transfer.

[83] For this access, DPS uses twenty-two Telex and 327X terminals. These consist of three TELEX 278 terminals, one TELEX 046 terminal, three TELEX 078 terminals, seven TELEX 1471 terminals, one IBM 3268 printer, four TELEX 281B printers, one TELEX 287D printer, two TELEX 1201 printers, five Mannesmann-Tally MT87 printers, three Mannesmann-Tally MT130 printers, two TELEX 1191B terminals, and two TELEX 276 terminals.

[84] APD has one IBM 3274 Control Unit, one IBM 3290 terminal, one IBM 3276 terminal, one IBM 3191 terminal, and one TELEX ISYS 90 terminal.

[85] APD bought thirteen Intel-based DeskTop workstations for special applications. All of the DeskTop workstations are connected to the APDI Net.

[86] The APDI Net workstations consist of 106 Macintosh processors, fourteen Intel processor devices, and a mix of seventy-two printer devices.

d. APD Standard Software.

APD has standard software for its mainframe,[87] minicomputers,[88] and microcomputers.[89]

3. Future Technology Development Plans.

Because of the problems it has been experiencing with PLIMS, APD is issuing an RFP for new application software. The department is requesting an improved Police Records Management System (PRMS) that will interface with the existing PLIMS CAD and APSIN, a Property and Evidence Tracking System, and a CAD system. APD prefers to keep its existing hardware and CAD system, but it is willing to consider a total system replacement. Although arrest information could be transferred from APD to APSIN through the proposed PRMS connection, the content and format of data transferred has not been discussed.[90]

[87] APD's mainframe software consist of a Unisys A Series operating system (MCP 3.8 or above), application development (LINC II 14.5 or above), a data base management system (DMS II), a communications system (System/Coms), an editor (CANDE), job control (WFL), and a data base query tool (DARGAL).

[88] The APD's minicomputer software is VAXstation 3100, operating system (VMS), a data base management system (ArcInfo 6.0 or above), and communications (DECnet).

[89] APD's Apple Macintosh Systems microcomputer software consists of an operating system (System 7.0.1 or above), application licensing (KeyServer), data base applications (FoxBase, FileMaker Pro), word processing (Microsoft Word), Spreadsheet (Microsoft Excel), E-mail (Microsoft Mail), scheduling (Meeting Maker), graphics (MacDraft, SuperPaint), presentation (Power Point, Harvard Graphics), desktop publishing (Pagemaker), desktop communications (MicroPhone II), text retrieval (Sonar Pro), MT emulation (CTCBridge), file backup (Fastback Plus, File Recovery), project management (Project Scheduler 4), spooler (SuperLaser Spool), scanning (PhotoShop), OCR (Omni Page Professional), and a network (AppleShare, AppleTalk Remote Access, TCP/IP). INTEL-based systems include an operating system (MS-DOS 5.0, Windows 3.1), application development (Clipper), data base applications (FoxPro, FileMaker Pro), word processing (Microsoft Word), file backup (Fastback, Unisys Tape Utility), file recovery (Norton Utilities), anti virus (Viruscan), PC to Macintosh communications (Timbuktu), MT emulation (CTCBridge), and a network (Novell, AppleShare, TCP/IP).

[90] Although APD would like direct access into OBSCIS in order to locate prisoners, and into the court criminal system to check case status, connectivity will not be possible until these systems are replaced.

The cost of APD's new systems will vary by vendor and whether the existing software can be salvaged to use with the new system. APD feels confident that it will have the funds to implement the selected solution.

J. Municipal Prosecutor

The Anchorage Municipal Prosecutor's Office prosecutes cases initiated by the Anchorage Police Department where municipal ordinances are cited, or from the Troopers when they cite a municipal ordinance because there is no corresponding state statute. Any felony cases are transferred to the Department of Law.

This agency only has word processing programs on its PC's, but is trying to develop a case management system using the Spokane, Washington prosecutor's system. They would like a direct connection to APSIN to retrieve CCH and driver's license data, and direct access into OBSCIS to retrieve prisoner location information. They currently have a dedicated terminal into APSIN for CCH retrieval.

All cases presented to them by APD are on the Criminal Case Intake and Disposition (CCID) form, a copy of which is eventually forwarded to the DPS Records and Identification Section in Juneau.

K. Other Local Police Organizations

Local police departments need to inquire into APSIN, and do so through dedicated terminals that also are used to enter arrest information. Access is through the current SNA network. However, the Alaska Chiefs of Police Association currently is concerned about the completeness and accuracy of the CCH repository. In the future, the chiefs would like to be able to inquire about prisoner location, juvenile status, and fish and wildlife case dispositions that are not currently stored in the criminal history repository. Also, the chiefs support the legislation mandating fingerprinting, and the future promulgation of regulations concerning the submission of case and offender information.

L. Alaska Judicial Council (AJC)

The AJC is a constitutionally created judicial branch agency independent of the court system. Although the AJC does not create criminal justice information in its day-to-day operations, it has a long-standing interest in the criminal justice system by virtue of its constitutional mandate to conduct studies to improve the administration of justice in Alaska. Since 1973, the AJC has worked with criminal justice agencies, using their data to review sentencing and bail practices, evaluate agency policies, and advise the legislature on legislation.

The AJC uses criminal history records for its other two tasks as well. The constitution requires the Council to nominate applicants for all state judgeships to the governor.[91] Statutes require the Council to evaluate each judge standing for retention and to provide the evaluations to the voters. For both tasks, the Council reviews criminal history records, along with a wide variety of other information.

While serving as staff to the Alaska Sentencing Commission from 1990-1993, the AJC established a statistical/relational criminal justice data base that tracks offenders and events through the entire criminal justice process (the Justice Unified Statistical Data Base, or JUSDB).[92] The JUSDB contains three primary files: offender information, event information and case information.[93] The event file contains information about offense, disposition and sanction, criminal history, NCIC and FBI reports, pre-sentence report data and revocations. The offender file contains static demographic information such as gender and race. The case file contains multiple charge records for individual cases. Although the Sentencing Commission has finished its work, the AJC's Research Analyst continues to update and improve the data base.

[91] The governor must appoint a judge from the list of two or more nominees sent by the Council.

[92] Creating the data base was a two-step process. First, selected information was taken from the DPS, DOL and DOC systems. Those data were cross-indexed and merged into a single relational data base. Secondly, the composite data base was expanded with information taken from original paper files, such as pre-sentencing reports and court judgment forms. The second stage filled information gaps and validated the accuracy of the computer data.

[93] Where the same information appeared in two or more files, disparities between the files were analyzed using the merging process. Although only one field generally was incorporated into the merged data base, no data were lost because all original data remained intact.

The Research Analyst and other AJC staff use the data base to answer questions from the legislature, the public, and criminal justice agencies. In addition, individual departments can use the system to update their computer systems.[94] The data base has provided statistical information to aid policymakers' decisions regarding, for example, characteristics of certain types of offenders, existence of sentencing disparity, impacts from changing sentencing statutes, and resource allocation issues. The data base also provides historical information useful in analyzing longer-term trends or impacts of changes on the criminal justice system as a whole. The JUSDB is the only integrated system in Alaska containing the information necessary to comprehensively address sentencing issues.

M. Existing Coordination Efforts

For the past several years, Alaska's criminal justice agencies have been working to coordinate their computer information systems. This process began with recommendations from the Alaska Sentencing Commission. These recommendations focused on collecting data from the criminal justice agencies into a data base to aid policy makers (as discussed in the preceding section); developing a court case management system; increasing the use of common incident and person identifiers throughout the criminal justice system; and developing communication between information systems so that data could be shared rather than being repeatedly re-entered.

The Sentencing Commission also recommended that its coordination efforts be continued after the Commission ended. Three separate criminal justice agency working groups have worked on these issues over the past year. They are the Criminal Justice Working Group (CJWG), the Criminal Justice Coordination Policy Group, and the Technical Users' Group. The Alaska Judicial Council has taken the lead in facilitating these groups.

The CJWG was re-constituted and appointed as an official task force in September of 1993 by Governor Hickel. The group, composed of criminal justice department

[94] For example, APSIN lacks data regarding case disposition once a case is referred to the prosecutors. Key variables could be returned to APSIN to update its records without having to match cases across systems.

commissioners, the court system, legislators, and local law enforcement, meets approximately once a month. The members of the group are briefed regularly on computer coordination efforts and they make policy decisions affecting computer coordination. For example, they recently discussed and recommended that the governor pursue the mandatory fingerprinting legislation discussed in Appendix C. The group also considers the fiscal needs for the systems. The CJWG's focus is of course much broader than just computer coordination issues.

The CJWG established a Policy Group to focus on the computer information system issues. The committee has a membership of deputy commissioners and division heads from each of the criminal justice agencies. Interested legislators are informed of meeting dates and actions taken by the group. This policy group developed the RFP for this report, assisted in evaluating the proposals received, and met with the consultants. The Policy Group also considers action on recommendations from the Technical Users' Group, including recommendations about standard data elements and formats.

The Technical Users' Group had been meeting for almost two years. Members have agreed on standard formats for several common data elements, are reviewing the data elements for the CCH, and are continuing with work in implementing system-wide use of person and incident identifiers. The group also has discussed the need for tracking individual charges and other technical aspects of coordinating operation of the computer systems.

The legislature has supported and even insisted upon these coordination efforts. One year ago the legislature appropriated $75,000 to the Judicial Council and instructed the Council to work with the criminal justice agencies to develop a plan to coordinate their computer information systems. This report is the result of this project.

Chapter II

Information Quality Assessment

This chapter explains how each criminal justice agency uses criminal history records, and then assesses the quality of the criminal history record information as it relates to sharing information among Alaska agencies in an integrated justice system. Data quality is measured by the completeness, accuracy, timeliness, and availability of the data. This section first describes how the criminal justice agencies use criminal history records (including key federal initiatives that will affect Alaska's criminal justice system), and then analyzes the data quality of criminal history record information in Alaska.

A. Use of Criminal History Records

All criminal justice agencies rely every day on criminal history records to process their own caseloads. In particular, the criminal history records of repeat offenders are vital to decision-making for all users.[95] This section explains how each criminal justice agency in Alaska needs timely access to complete and reliable criminal history record information.

1. Police

Perhaps the most important police use of the criminal history record is on the street when making a stop. Knowing the suspect's prior record, especially violent behavior, can be vital in protecting the safety of the public and the officer. Moreover, the criminal history record tells the officer that a crime has been committed if a person carrying a concealed weapon has a prior felony conviction.[96]

The criminal history record also is vital to investigative work. Police use the record to detect crime patterns or compile lists of suspects, eliminating those the criminal history record accurately shows were incarcerated at the time of the offense. A current,

[95] In most states, over two-thirds of persons arrested have prior criminal history records.

[96] AS 11.61.200 makes possession of a concealed firearm by a convicted felon a Class C felony, within a specified time period.

accurate criminal history record facilitates serving warrants and making arrests by providing the last-known address, especially if that person is on parole or is a registered sex offender.

2. Prosecutors

The prosecutor uses the criminal history record when filing an information or an indictment, making recommendations about bail, enhancing charges for habitual or repeat offenders,[97] assisting in plea bargaining, and making recommendations about sentencing and parole. The criminal history must be available, complete, and accurate in order for the prosecutor to give timely notice of the intent to seek enhanced sentencing for an offender, and to give notice of intent to upgrade an offense class for a habitual or repeat offender.

3. Courts

Courts use criminal history records at the beginning, at the end, and all throughout criminal cases. At the beginning, criminal history records are important to decisions about bail or other release before trial, particularly if the criminal history shows a pattern of violent or sexual offenses that indicate the offender poses a danger to the public.[98] Too often, criminal history records are not available or complete enough to help a judge decide whether and under what conditions an offender might be released. Moreover, because decisions about bail often must be made within 24 hours of arrest, the information must be timely.

The importance of positive offender identification by fingerprint comparison at the pre-trial release stage cannot be overstated. If the person arrested has used an alias, he or she may escape identification under a name search of the criminal history record

[97] Many states, including Alaska, have laws upgrading the class of an offense based on prior criminal activity for a particular offense. For example, AS 11.46.130 provides for upgrading theft charges to a Class C felony for theft of property valued at $50-500, if the offender has been convicted and sentenced for theft or concealment twice in the last five years. AS 11.46.140 provides for upgrading of theft charges to a Class A misdemeanor for theft of property valued under $50, if the offender has been convicted and sentenced for theft or concealment twice in the last five years.

[98] AS 12.30.020(c)(8) permits use of prior criminal history to impose conditions on release from custody, or to secure an appearance, or to protect the public from the offender.

data base. Also, knowing that an offender has failed to appear at a hearing, violated a condition of bail, or committed a crime while on bail for another arrest is important to the judge's decision at any point in the process.

Courts must know an offender's prior criminal record when sentencing presumptively.[99] In Alaska, sentences may be enhanced by the number of felony convictions, as well as by the number of previous incarcerations. Alaska currently is debating whether to join other states in enacting a "three-strikes-and-you're-out" law, that would mandate life sentences without possibility of parole for serious repeat offenders.

Courts receive prior criminal history information from reports prepared by pre-trial services, from prosecutor filings, and from pre-sentence reports developed by parole and probation agencies. Courts often are allowed to use certain types of prior criminal activity to show a defendant's motive, intent, or patterns of behavior, or to assess a witness's credibility or veracity.

Finally, courts use prior criminal history records to make decisions about whether and under what conditions to place an offender on probation. The criminal history can help the judge decide whether the offender poses a threat to the community or can be trusted to adhere to the terms of the probation. Also, the criminal record can assist the judge in determining eligibility for and conditions of parole.

4. Corrections

Corrections uses the criminal history record to help make decisions about inmate classification, probation, parole, time accounting, and for background checks on visitors, employees, delivery persons and others who have access to correctional facilities. Corrections must assign offenders to programs based on prior convictions, especially sex offenses.[100] DOC also needs reliable and complete information on the offender's conditions of incarceration. Decisions about discretionary parole depend to a large

[99] AS 12.55.155 permits courts to significantly increase a sentence where the offender repeatedly has committed offenses of a particular kind. AS 12.55.125, .145 and .175 all provide for enhanced presumptive sentences for repeat felony offenders.

[100] AS 33.30.091.

degree on an offender's criminal history.[101] Finally, Alaska corrections officials have underscored the importance of the criminal history record in making sure that every sentence has been served before an offender can be released.

B. Federal Initiatives and Legislation Affecting the Criminal History System in Alaska

Federal initiatives and legislation are placing greater emphasis on the availability and quality of states' criminal history record information. Federal legislation includes the Brady Handgun Violence Prevention Act, the National Child Protection Act, and the Immigration Act of 1990. Federal initiatives include the BJS Criminal History Record Improvement Program, the BJA Block Grant Funds for Data Quality Improvement, the Integrated Automated Fingerprint Identification System (IAFIS), NCIC 2000, and the FBI/BJS Recommended Voluntary Standards for Improving the Quality of Criminal History Record Information. These are discussed below.

1. BJS Criminal History Record Improvement Program

Section 6213 of the Anti-Drug Abuse Act of 1988 requires the Attorney General to develop a system for the immediate and accurate identification of felons attempting to purchase firearms. On November 20, 1989, the Attorney General made recommendations to Congress for implementing this statute, citing the problem of incomplete and inaccurate criminal records as a major obstacle to achieving positive identification of felons.

Accordingly, the Attorney General directed the FBI, in conjunction with the Federal Bureau of Justice Statistics (BJS), to develop voluntary standards for improving the data quality of the nation's criminal history records, and directed the Bureau of Justice Assistance (BJA) to allocate $27 million out of its Anti-Drug Abuse Discretionary Fund ($9 million each for FY 1990, FY 1991, and FY 1992) to assist states in complying with the BJS/FBI standards.

[101] AS 33.16.090 and .100 place limits on discretionary parole for offenders convicted and sentenced to enhanced terms as habitual offenders. AS 33.16.110 requires the parole board to consider the sentencing court's presentence report, including the offender's criminal and juvenile history.

All $27 million has been awarded by the Federal Bureau of Justice Statistics; all states, along with the District of Columbia, American Samoa, and the Northern Mariana Islands, have participated in the program.

2. BJA Block Grant Funds for Data Quality Improvement

The Crime Control Act of 1990 amended Part E of the Omnibus Crime Control and Safe Streets Act to require each state to allocate at least 5% of its Edward Byrne Memorial State and Local Law Enforcement block grant award for the improvement of criminal history records.[102] The improvements should, at a minimum, result in criminal history records with final dispositions for all felony arrests, the full automation of supported criminal histories, and compliance with the voluntary reporting standards of the FBI, as directed by the Attorney General.

States have used the Byrne block grant funds to improve criminal history records. However, the block grant program has been "zeroed out" of the President's budget for fiscal year 1994-95.

3. Reporting of Alien Convictions to the Immigration and Naturalization Service (INS)

The Immigration Act of 1990 requires each state to assure as part of its application for Formula Grant funds that it has established a plan under which the state will provide to INS, without fee, the conviction records of convicted aliens. To be in compliance with the Act, states must ensure that their criminal history record systems capture data on the offender's place of birth and country of citizenship to determine alien status. Final convictions include both felony and misdemeanor convictions related to aliens or suspected aliens by a court of competent jurisdiction for which all direct appeal rights have been exhausted or waived or the appeal has lapsed.

The reporting requirement was designed to assist both INS and state and local governments to deal with convicted aliens. INS estimates that 10% of the inmates in prison are illegal aliens. Once released from prison, they can be deported, thereby reducing recidivist crime and the associated costs of further prosecution and incarceration.

[102] This set aside has amounted to about $70,000 per year for Alaska.

In 1991, Congress amended the Immigration Act to allow states to provide INS with notification of the conviction of a suspected alien and provide a certified copy of the conviction record later, if requested by INS. The states must, to be in compliance with the Act, ensure that their criminal history record systems capture data on the offender's place of birth and country of citizenship to determine alien status.

The alien reporting requirement must be included in the criminal history records improvement process, and care should be taken to ensure that the planning process identifies the best way to accomplish this mandate.

4. Integrated Automated Fingerprint Identification System (IAFIS)

IAFIS is a "paperless," computerized criminal history and fingerprint identification system under development by the FBI's Criminal Justice Information Services Division (FBI-CJIS). The three components of IAFIS are the Interstate Identification Index (III), Identification Tasking and Networking (ITN), and the Automated Fingerprint Identification System (AFIS). When fully implemented, IAFIS will offer the capability of eliminating paper fingerprint cards at every step of the identification process. The ITN will handle workstations, work flow control, telecommunications, and fingerprint image files to support paperless identification processing.

States participating in IAFIS will use live-scan fingerprint technology at arresting and booking agencies. (Card-scan technology can also be used to capture fingerprints.) The live-scan fingerprint images will be processed by regional AFIS workstations and transmitted to the state identification bureau for positive identification. If positive identification is not achieved at the local or state level, then fingerprint data, along with personal descriptor data, will be electronically sent to the FBI's IAFIS. The FBI will then transmit a response of hit or no-hit to the local agency.

The process should take less than two hours. This will allow law enforcement agencies to positively identify persons in custody before releasing them from custody or from bail hearings. Coupled with the criminal histories from other states available through III, IAFIS will be able to identify persons using aliases as well as fugitives from justice.

Individual states can decide on their level of participation in IAFIS. At the minimal level of participation, states will not have to modify their systems to participate. However, those states that do modify their system to take full advantage of the benefits of IAFIS will witness significant improvements in identification and processing capabilities. These would include greater identification accuracy, faster response time to identification inquiries, and a reduction in manual labor related to identification processing. Alaska will not be able to achieve the level of IAFIS participation required for the timely and accurate identification of felons using the current AAFIS.

5. NCIC 2000

The FBI's NCIC 2000 program will result in an upgrade of the National Crime Information Center's telecommunications system to allow for a paperless transmission of identification information, including criminal histories, records of wanted and missing persons, and records of stolen property. The new system also will support the electronic exchange of graphical information, such as mug shots, tattoos, and signatures.

Improved capabilities anticipated under NCIC 2000 include:

- Addition of image processing.
- Addition of automated fingerprint processing and identification.
- Automation of NCIC routine functions, such as validation, on-line hit confirmation requests, and collection of benefits information.
- Access to new data bases, including convicted persons on supervised release, SENTRY.
- Access to external data bases, including the National Incident-Based Reporting System (NIBRS)/Uniform Crime Reporting (UCR), and potential access to the Canadian Police Information Center (CPIC).
- Automatic collection of statistics for system evaluation.

- Relational data base ad hoc query capability to associate multiple records with the same criminal or same crime.

As part of the solution for NCIC 2000, Harris Corporation and Printrak International have developed new technology that allows law enforcement officers to get fingerprint identification during field stops.[103]

6. National Child Protection Act

H.R. 1237, the National Child Protection Act (known also as the Oprah Winfrey Bill) requires a national instant background check of individuals seeking employment in the child care field. As with the Brady Bill, the act mandates that states achieve an 80% final disposition reporting rate in child abuse cases that have occurred in the previous five years.

The act also provides $20 million in grant funds to assist states in the fiscal years 1994-1997 in improving criminal history records so that they can comply with the mandates of the legislation.

7. Brady Handgun Violence Prevention Act

Enacted on November 30, 1993, as Public Law 103-159, the Brady Bill imposes a five-business-day waiting period on the sale of a firearm. The Brady Bill took effect on March 1, 1994, and requires states to use the five-day waiting period to conduct a name search of centralized criminal history record data bases to determine if the purchaser has a prior felony record.

The act also requires the Attorney General to develop a National Instant Check System (NICS) to expedite criminal history record checks for firearms purchasers. NICS will require on-line participation by the states and significant improvements in state criminal history records programs. Specifically, states would have to achieve an 80-

[103] This technology uses an ISP Card, which will be implemented in the MIU in patrol cars and workstations. This PC-based card will extract fingerprint minutiae and perform compression/ decompression tasks at 128 MIPS.

percent disposition reporting rate for five previous years. NICS must be operational within five years of the enactment date.

8. FBI/BJS Recommended Voluntary Standards for Improving the Quality of Criminal History Record Information

Section 6213 of the Anti-Drug Abuse Act of 1988 required the Attorney General to develop a system for the immediate and accurate identification of felons who attempt to purchase firearms. In November of 1989, the Attorney General advised Congress of his recommendations for implementing the provisions of the statute, citing the problem of inaccurate, incomplete, and inaccessible criminal history records as a major obstacle in implementing the legislation.

Accordingly, the Attorney General directed the FBI, in conjunction with the Bureau of Justice Statistics (BJS), to develop voluntary reporting standards for state and local law enforcement. The Attorney General further directed that since the most urgent need is to identify criminals, the voluntary standards should focus on enhanced recordkeeping for all arrests and convictions made in the last five years.

The ten FBI/BJS Voluntary Standards for Improving the Quality of Criminal History Record Information are:

1. Every state shall maintain fingerprint impressions or copies thereof as the basic source document for each arrest (including incidents based upon a summons issued in lieu of an arrest warrant) recorded in the criminal history record system.

2. Arrest fingerprint impressions submitted to the state repository and the FBI Identification Division (ID) should be complete, and shall at least contain the following data elements: date of arrest, originating agency identification number, arrest charges, a unique tracking number (if available), subject's full name, date of birth, sex, race, and social security number (if available).

3. Every state shall ensure that fingerprint impressions of persons arrested for serious and/or significant offenses are included in the national criminal history records system.

4. All disposition reports submitted to the state repository and the FBI ID shall contain the following: FBI number (if available), name of subject, date of birth, sex, state identifier number, social security number (if available), date of arrest, tracking number (if available), arrest offense literal, court offense literal, and agency identifier number of agency reporting arrest.

5. All final disposition reports submitted to the state repository and the FBI Identification Division that report a conviction for an offense classified as a felony (or equivalent) within the state shall include a flag identifying the conviction as a felony.

6. States shall ensure to the maximum extent possible that arrest and/or confinement fingerprints are submitted to the state repository and, when appropriate, to the FBI Identification Division within twenty-four hours; however, in the case of single-source states, state repositories shall forward fingerprints, when appropriate, to the FBI Identification Division within two weeks of receipt.

7. States shall ensure to the maximum extent possible that final dispositions are reported to the state repository and, when appropriate, to the FBI Identification Division within a period not to exceed ninety days after the disposition is known.

8. Every state shall ensure that annual audits of a representative sample of state and local criminal justice agencies shall be conducted by the state to verify adherence to state and federal standards and regulations.

9. Whenever criminal history record information is collected, stored, or disseminated, each state shall institute procedures to assure the physical security of such information, to prevent unauthorized access, disclosure or dissemination, and to ensure that such information cannot be improperly modified, destroyed, accessed, changed, purged, or overlaid.

10. Every state shall accurately identify to the maximum extent feasible all state criminal history records maintained or received in the future that

contain a conviction for an offense classified as a felony (or equivalent) within the statute.

The standards have become the goal of all state criminal history record improvement plans filed with the U.S. Department of Justice.

C. Data Quality of Alaska Criminal History Record Information

This section assesses the quality of the criminal justice information available in Alaska. This assessment measures the completeness and accuracy of the available data, as well as the timeliness with which the data are available to users. This analysis is based on a review of literature on the justice agencies, on in-depth structured interviews, and on findings of the *Baseline Assessment* of Alaska's criminal history record processing conducted by the SEARCH Group (March 31, 1993).

1. Overview of Data Quality

Generally, Alaska's criminal history records information is neither accurate nor complete enough to meet users' needs. Nor are the data available in a timely manner. Critical decisions that should be supported by complete records of arrest and dispositions are too frequently made without the data. The agencies generally agreed that they do not have enough data, and that the data they have often are inaccurate. Users also noted that they lack mechanisms for sharing data.

Agencies cited various reasons for the data quality problems. The most common culprits included lack of staff resources to enter the data, lack of modern technologies to capture and exchange data, redundant data entry between agencies that leads to data entry errors, the inability of different data bases to exchange data, lack of standardization in data elements, and lack of a clear sense of the roles and responsibilities related to information sharing.

On the positive side, users agreed that the Arrest Tracking Number (ATN) increases data quality, especially in linking arrests and dispositions. All contributing agencies share a spirit of willingness to address these problems. The Criminal Justice Information Systems Technical Users' Group and the Computer Coordination Policy Group have addressed and resolved a number of key issues at their regular meetings.

Other accomplishments include the recent refinement of the ATN to include a check digit to reduce data entry errors, development of formats for transmitting shared data elements between agencies, and a review of the key data elements of the criminal history record.

2. *Analysis of Completeness, Accuracy, Timeliness and Availability of Data*

a) Completeness.

The state has reasonably complete arrest reporting information, including felony flagging for convictions. However, the state lacks fingerprint support for arrest records. Also incomplete is information on prosecutors' decisions to decline to prosecute.[104] Final court dispositions were found to be 86% complete, a high level. Finally, DOC does not report the receipt and release of prisoners to the criminal history repository.

b) Accuracy.

The criminal history record reports arrests accurately. Because the agencies do not track charges yet, it was difficult to assess the accuracy of arrests and dispositions. For key data elements of the court disposition,[105] the data are accurate over 95% of the time.

c) Timeliness.

Law enforcement reports arrests promptly through an automated process. Fingerprint cards take too long, fourteen days after DPS receives the cards. Prosecutors do not report the "decline to prosecute" cases quickly, but DPS enters the dispositions as soon as they receive them. DPS does not receive final court dispositions promptly; this process averages forty days. Final disposition entry into the CCH also was slow. Because felony dispositions receive prompt attention, staff enter the into the CCH quickly.

[104] Although DPS and DOL are trying to improve reporting through automation, the inflexibility of the PROMIS system has hampered their efforts thus far.

[105] Key elements include court name, charge literal, disposition, and sentence.

d) Availability.

Decision-makers, ranging from police officers to judges, cannot get the data they need about offenders when they need it during the justice process. The state should expand the current criminal history record to include additional data elements that will allow users to make decisions quickly and reliably. Chapter VI of this strategic plan recommends an expanded set of data elements for the state of Alaska's criminal history record.

3. Conclusions

Alaska must have complete, accurate, timely and available criminal justice information to integrate its justice information systems. Lacking this, Alaska cannot meet the operational needs of its criminal justice agencies, nor can it participate in the national programs explained in Part B above, which require accurate and reliable data from the state.

The lack of an integrated technology architecture that would support the collection, maintenance, and sharing of information lies at the heart of Alaska's data quality problems. Currently, Alaska's criminal justice information systems can not communicate with each other. Moreover, DOL's PROMIS system and DOC's OBSCIS system could not at present share in an integrated system because of their severe technical limitations.

The Alaska Court System is developing a court case management system that will use state-of-the-art technology. DPS operates stable mainframe technologies that permit other agencies to interface with their systems. Using this mainframe architecture as the model for an integrated solution would be costly. In the long run, however, DPS plans to shift its operations from the mainframe to a client/server architecture, beginning this migration with its Trooper Case Management System. Finally, justice system integration cannot occur unless the Department of Administration implements a robust, multi-protocol statewide backbone network to support it.

Chapter III

The Need for a Policy Framework To Develop State Information Technology

Alaska must establish a policy framework for acquiring, implementing, and managing information technology in its justice system. Every agency needs criminal history records, from arrest through to the final decision to release an offender from supervision. Present criminal history records lack complete, accurate data about the offender and the events in the criminal case. As a result, many participants -- police, prosecutors, judges -- cannot make the best possible decisions that protect the public. Further, these problems come in the context of intense pressure to reduce public spending.

The diverse agencies making up the criminal justice system, including law enforcement, prosecutors, courts, defense attorneys, and corrections, must share information about offenders and cases. At present, much of the sharing occurs through transmitting written information on paper, small parts of which may eventually be entered into a computer data base. The process takes time, and the pieces of paper or the information can be lost or misunderstood or misread. Agencies do not record information in the same format, making matching of records between one agency and the next difficult or impossible.

In order to address these problems, agencies must agree on a set of policies that govern who collects the information, how it is stated, where and how it is recorded, and when and with whom it is shared. The policies should cover not only agency staff responsibilities but standards for the purchase and maintenance of the computers, software, and other technology needed to accomplish the sharing that agencies have agreed is needed. Absent the policy framework and authority for individual agencies to carry out their tasks, we do not believe that any integration effort will succeed. The state must actively lead to build the framework for integrating heterogenous systems. A framework for establishing those policies is the subject of this chapter.

A. Oversight

The state must assign oversight responsibility for establishing and maintaining policies governing criminal justice information. Individual agencies should retain control over the acquisition and operation of their own equipment, staff and programs. The oversight authority would have a mandate to:

- Assess the technical, managerial, and economic feasibility of agencies' proposals for new acquisitions;
- Establish state-level strategies;
- Decide on the equipment to be purchased and used at the statewide level for sharing information;
- Help agencies plan for their in-house acquisition and use of technology;
- Coordinate the planning and justification (to the legislature and executive branch budget agencies) of multi-department projects;
- Assure that agency proposals match with the overall direction that the state has chosen for managing information and building a technological infrastructure;
- Encourage and advocate proposals from agencies that realistically can improve state programs substantially.

We cannot dictate who will assume this essential oversight role. We can, however, suggest where the state might vest such authority in existing agencies.

- **Department of Administration Division of Information Services**

The Division should develop standards for client/server and distributed systems (see Appendix D) and, after approval by TIC (see the following paragraph), publish those standards. The Division also should assist other agencies in planning new system technologies, and provide training in these technologies.

- **Telecommunications Information Council (TIC)**

TIC should take responsibility for approving client/server and distributed system standards, for managing the state's technology resources, and for providing policy guidance to all state agencies.

- **Criminal Justice Working Group**

The Criminal Justice Working Group, composed of cabinet-level officials from the operational agencies, should resolve inter-agency policy issues related to information sharing. It should use the Judicial Council staff to the degree possible to facilitate activities.

B. The Approach to a Policy Framework

The state cannot predict the future for information technology with certainty. However, it can follow a set of principles that will help create flexible, cost-effective policies for acquiring, using and managing technology. The principles should focus on establishing statewide standards that permit agencies to meet present needs and respond to new demands for information and public services. The specific principles that the policy framework should incorporate are:

1) Each state agency should set up a technological infrastructure that serves as a foundation for current and future information sharing and use. Each agency, therefore, must participate as a partner in a statewide technical architecture.

2) The system must acknowledge the autonomy of individual agencies, leaving each free to use the programs best suited to carrying out its responsibilities.

3) Both the state and the individual agencies should use existing infrastructure to the maximum extent possible when responding to newly identified needs and opportunities.

4) Individual agencies should use existing resources as much as possible, including state backbone networks, multi-agency data centers, and existing sources of data.

5) Agencies should share data so that they can improve services to shared clients, resolve shared problems, avoid duplicating data collection and record keeping, and reduce costs.

6) The state should establish and maintain standards for technology that apply to all agencies, when adopting particular standards will further the state's interest as a whole.

C. The Elements of a Policy Framework

The policy framework should provide guidance for the state as a whole and for individual agencies. The policies in the framework should set an approach to criminal justice information systems that structures how agencies plan for, purchase, implement and maintain both the individual parts of the systems and the shared information. The key elements include policies for planning, feasibility studies, project management, evaluation, and security and risk management.

1) ***Planning:*** Each agency should create a plan that identifies its needs for information, defines the objectives for managing information, and decides how the agency will use technology to meet its needs and objectives. Executive, technical and program staff all should participate in planning. The agency should document periodically how the plan is being implemented.

2) ***Feasibility Studies:*** Each agency should report to the legislature and the state oversight agency about the need for a proposed technology purchase, its benefits, its connections with existing resources and infrastructure, and how it meets the standards set for criminal justice information systems. Agency management, the legislature and the state oversight agency can use the feasibility study to evaluate the project, set priorities among competing projects and allocate the state's resources.

3) ***Project Management:*** Once the agency begins to acquire, install and use the new technology, the policy framework should require that the agency use proven management policies for the particular technology. Agencies should report to the state oversight agency regularly about progress. The level of reporting required should be tied to the complexity, risk and costs involved in each project.

4) ***Evaluation:*** Throughout the operational life of a system, the agency should evaluate its benefits, costs, and ability to meet the objectives initially set for that system. The agency also should consider how the technology fits into the changing needs of the public and clients served by the agency. The agency should use the evaluation findings in revising the overall agency plan, as well as sharing its experience with other state agencies.

5) ***Security and Risk Management:*** Loss or damage to the state's information assets -- its files and data bases, software, equipment and facilities -- jeopardizes the state's ability to provide essential criminal justice service and protect public safety. The policy framework should guide agencies in the classification, use and protection of automated files and data bases, and equipment. An Information Security Officer in each agency should work with agency staff and other agencies to coordinate security. Each agency also should create a recovery plan to help resume operations in case of a disaster. Agencies can cooperate in preparation of the recovery plans, and the state oversight agency should review and coordinate the planning process.

D. Conclusion

The technology infrastructure that is the subject of the policy framework includes all of the mechanisms needed to collect, maintain and deliver criminal justice information. The information infrastructure, like a community water system or electrical grid, includes the people who build, use and maintain the system as well as the physical parts of the system such as the pipes, roads or computers and their connections. Once the system exists, the agency responsible for it can expand or enhance it to serve new customers and needs without building an entire new system to respond to each new demand.

The state built its current technology infrastructure agency by agency, piece by piece, over the past two decades. It can combine many of the pieces, with the guidance of the policy framework, into new configurations that better use the state's resources. The state will benefit more by replacing other pieces, retraining staff in use of new technologies, and designing better-coordinated approaches that minimize individual entry of data and maximize the opportunities for sharing data electronically. In the process of re-thinking the computerized information systems for individual agencies and for the criminal justice system as a whole, the state can gain economies of scale, and can create new services and products, such as more accurate and useful criminal history records. Overall, establishing a policy framework for acquiring and using criminal justice information systems will let the state respond to its citizens more effectively and more quickly.

Chapter IV

Business Process Re-engineering

Before the state can begin the work of choosing new technologies for criminal justice information systems, and before it can integrate the existing systems into new frameworks, agencies must define what their work includes and how the desired data can best be shared. Ten or twenty years ago, this process might have been referred to as master planning; today, many describe it as "business process re-engineering." The term simply describes a process of thinking through what work each agency does that requires information, how the agency gets (or could get) the needed information, and what interactions with other agencies are required in order for the agency to get or give information. The process results in a plan for the two aspects of information technology. The application architecture describes all of the activities and products necessary to completely automate an organization's work. The technology architecture defines and ranks by priority all of the hardware, software, data bases, networks and other components needed to support the applications chosen. The process has the advantage of emphasizing the departments' needs and work rather than focussing exclusively on technology.

In Alaska's criminal justice system, both the Department of Public Safety and the Court System have done this type of thinking during the past several years. The Departments of Law and Corrections have worked with their existing systems, making some revisions but not reviewing their entire operation. This chapter sets out the process for deciding what systems will suit the needs of the individual agencies, and the criminal justice system's needs for shared information. The agencies must do this work in order to submit proposals to the state oversight agency, draft budget requests to the legislature, draw up RFPs for new purchases, and begin to re-assign and re-train staff to install, operate, maintain and evaluate new systems.

A. Problems with the Current Technology Environment

The current environment, including the hardware and software installed, as well as the training of staff, affects the design of a new system. Existing problems include many different types of hardware and operating systems, both within and among agencies; inconsistent formats for entering, storing and transmitting data; various types of networks connecting the hardware and software; and data management staffs with varying missions and objectives.

1) ***Multiple Hardware and Operating System Platforms*:** The criminal justice agencies have acquired a variety of stand-alone and networked personal computer systems, in addition to their data bases and case management systems that reside on the state's mainframes. The agencies follow a nationwide trend shifting away from reliance on the mainframe to lower-cost, user-friendly PC systems. But this trend has costs as well as benefits. While the programs may meet the immediate needs of users, the systems may require substantial resources to use and maintain, especially when the varieties of systems proliferate. The individual agency and the criminal justice system as a whole may suffer because larger objectives cannot be met with the smaller system.

2) ***Inconsistent Data Formats:*** Each agency has developed systems to meet its own needs in-house. The result has been unique formats for entering even the most basic data, such as name, date of birth, social security number and offense charged. The unique formats greatly increase the difficulty of sharing data across different agencies. Often the information is re-entered manually, which greatly increases the chances of error and makes some important tasks, such as charge tracking, virtually impossible.

   Relational data bases such as SQL (Structured Query Language) set a standard syntax for data that maximizes the number of ways in which the data can be reached and shared. Other new products help translate data from one format to another. Both approaches help to resolve the problems created by the existing inconsistencies in the ways data are recorded.

3) ***Heterogeneous Networks:*** The agencies have networks as varied as the hardware and software acquired in the past ten years. Many of these networks can be tied to each other, and to the state's backbone networks, but the options can be bewildering in their complexity. The review of agency work and needs must consider carefully the costs and benefits of existing networks and the connections needed for maximum flexibility in the future.

4) ***Data Management Staff and Resources:*** Within each department, staff maintain the existing hardware and software, and take responsibility for planning to meet the agency's future needs. Typically, the professionals come from varied backgrounds, and because of the specialized requirements for their positions, are highly skilled in some areas but not others. The state has not had an overall approach to planning for criminal justice information systems or (until quite recently) any forum in which the agencies' professionals could meet to discuss common goals and needs. The review of the agencies' work must consider the existing skills of its staff, and how best to use or retrain these staff in new systems.

B. The Context for Business Process Re-engineering

Given current budgetary pressures, it is only natural that the legislature and administration expect agencies pursuing new automated systems to judiciously invest in new technologies that will help the agency operate more efficiently and still achieve its strategic business objectives. Recent advances in technology offer the opportunity to achieve this goal. They include:

- Powerful RISC processors and the widespread appearance of high-powered desktop machines which offer the promise of moving applications off expensive mainframe platforms.

- ANSI-standard, relational data bases which offer simplified access for ad hoc queries and decision support, while simultaneously providing enterprise-wide access and maintaining acceptable transaction response times.

- Network connectivity products that allow heterogeneous networks to be linked into large complexes of interconnected processors.

Many of these advances, however, raise significant possible problems that need to be addressed:

- Data base design trends have moved business rules into the data base and raised the importance of data base design and administration.

- The move to client server applications requires stronger control over personal computers, to ensure that desk-top configuration files, boards, communication software, etc., are compatible with the requirements of the client server applications.

- Security and network management have both become more complex in distributed/decentralized environments, increasing support resource demands.

- Many products touted as suitable for developing or supporting "mission critical" systems remain seriously inadequate, and prove dysfunctional when deployed in demanding processing environments.

- Development methodologies and assorted support tools have undergone radical change, making older approaches obsolete.

The re-engineering process must rely on state-of-the-art technologies, but at the same time be sensitive to the need to extract maximum value from existing legacy systems. When sensible, such systems should be retained and integrated with the strategic architecture. However, both the prosecutor and correctional operational systems appear to have little salvageability.

C. Conducting the Business Process Re-engineering

Alaska's criminal justice agencies, especially the Departments of Law and Corrections, need to re-examine the aspects of their work that require information in the context of their overall missions, their agency resources and their existing technologies before deciding what new technologies to acquire. They also need to work with other agencies in this process. The "business re-engineering process" uses a three-part method to do this work: assessment, strategy development and plan development. Figure 11, at the end of this chapter, diagrams the process.

1. Assess Needs

Departments take the first step in the re-engineering process by carefully assessing their needs. They must meticulously determine what agency objectives and needs any computer information system must address. This process basically breaks down into four steps:

a) Management reviews the department's overall objectives and framework with the staff responsible for re-engineering. The objectives include those set by the state's constitution and statutes, and those established by regulation and internal policy.

b) Project staff interview a cross-section of the Department of Law and Department of Corrections employees. The interviews should include administrative staff, professionals (e.g., attorneys, probation officers, institution superintendents), and technical and clerical staff. The interviews should focus not just on what information needs each group has, but also on what their actual work is, to better perceive what new information might be useful.

c) Based on the interviews and other available information, project staff create a business function model that defines all of the agency's business activities. For Corrections, this includes a wide range of activities, from those that protect the public directly by isolating offenders, to those that educate and inform various parts of the public (e.g., legislators, victims), to those that work with offenders in the context of various interest communities (e.g., presentence report writers, probation officers supervising offenders). For the Department of Law Criminal Division the primary business function is prosecuting offenders, but the division also drafts legislation, advises the legislature on proposed bills, and works with victims.

d) Based on the business model and other available information, project staff create a data model that describes the department's information needs. The model will include information needed internally to process cases or track offenders, as well as noting what information must be shared, or is most easily and accurately available from outside the department. The model should give some sense of when and where the information is needed, in what format, and subject to what restrictions (e.g., security, confidentiality).

Department staff will review the models and agree on their structure and content before moving onto the next phase.

2. Develop Strategies

The departments will meet with various staff in workshops to decide how they want to meet the information needs described in the models. The steps of developing the strategies include:

a) Design a structure for the staff organization that will support information systems within the agency;

b) Recommend an "ideal" technical architecture (e.g., specify the hardware, software, networks, and peripherals) that will collect, store and analyze the information needed;

c) Analyze the "gaps" that exist between the ideal situation and the recommended structures; and

d) Analyze the costs of implementing the ideal architecture.

Staff should work through this process without concern about cost during the first three steps. The department's business needs and priorities should shape the models and strategies. The department then can consider the different ways of meeting its needs, and accurately weigh the costs and benefits of each. The recommendations for the technology should serve during the purchasing phase as criteria for evaluating vendors and their products. Those that do not fit reasonably well with the recommendations should not be considered further.

3) Develop Plan:

Staff should meet again in workshop settings to create a project plan for acquiring and using the information systems recommended. They must agree on three types of plans:

a) Management plans that create the staff structures; that define policies and procedures for staff and data management; and that establish evaluation and monitoring procedures;

b) Technology plans that describe how the hardware, software, data bases, and network components will be put into place; and

c) Application plans that consider how information will move within the structures.

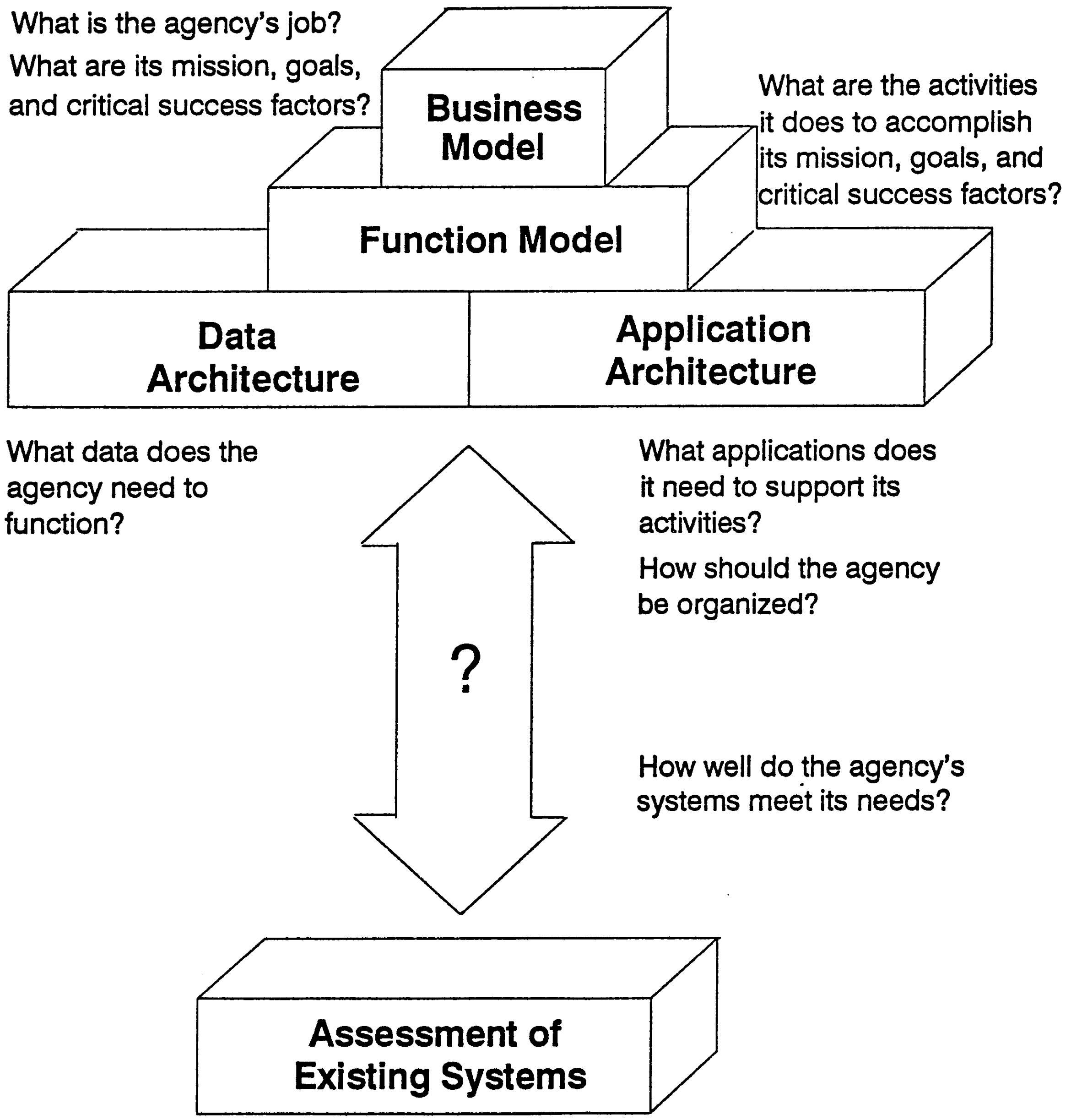
4) Product of Re-engineering:

The re-engineering process will produce a plan that describes the technology and staffing needed to support the departments' work. The report prepared should include chapters on each of the following topics:

a) macro-level cost/benefit analysis, and analysis of the impact of the plan;
b) staff organization, with roles and responsibilities specified;
c) information needed, and ways of obtaining it;
d) assumptions and constraints;
e) identification of the labor, material, and funds needed to implement the plan;
f) technology architecture recommended;
g) priorities for implementing the activities recommended;
h) plan and timeframe for implementing the activities.

FIGURE 11

SYSTEMS PLAN COMPONENTS


What is the agency's job?
What are its mission, goals, and critical success factors?
Business Model
What are the activities it does to accomplish its mission, goals, and critical success factors?
Function Model
Data Architecture
Application Architecture
What data does the agency need to function?
What applications does it need to support its activities?
How should the agency be organized?
?
How well do the agency's systems meet its needs?
Assessment of Existing Systems

Chapter V

Model for an Integrated Computerized Criminal History Record (CCH)

A. Introduction

Criminal justice personnel have debated the nature and contents of a state-level computerized criminal history repository since technology made the repositories possible in the early 1970s. The nation's focus on violent crime, combined with state and federal initiatives aimed at identifying felons have intensified the debate in the 1990s. Virtually every state suffers from under-reporting of arrest and disposition information, leaving state records inaccurate and incomplete. The U. S. Department of Justice recently estimated that only 17% of the criminal history records in automated systems have a final court disposition.

Criminal justice agencies cite inadequate staff resources, lack of good policies and procedures, lack of or inadequate automated systems, and lack of state statutes requiring timely, complete and accurate reporting of arrests and dispositions as the reasons for the low quality of criminal history records. A critical deficiency in the record itself underlies all of these reasons: the records do not provide the information the users need to make vital decisions about offenders. Even if all of the information that was supposed to be in a typical criminal history record were there, in a timely manner, for example, a prosecutor still could not go to the record to find out whether a given defendant had failed to appear in court after pre-trial release, whether the defendant had actually paid a fine imposed, or whether the defendant had previously been charged with (but not necessarily convicted of) violent behavior. Few state criminal history records provide timely information about the parole or release dates of an offender, information that victim notification statutes require.[106] Most do not have citizenship data, mandated by

[106] *See* Alaska Statutes 33.30.013. Prosecuting attorneys also are mandated by law in certain cases, if the victim so requests, to notify the victim of final case disposition, and the time and place of the sentencing hearing. *See* AS 12.61.015.

federal law which requires that convictions of aliens be reported to the Immigration and Naturalization Service.[107]

Alaska must re-construct its criminal history record to include the data that its users need to perform their jobs. The information entering and leaving the criminal history repository must be complete, accurate and timely. This chapter sets out the structure and contents of a model criminal case history repository for Alaska.

B. Possible Choices for Criminal History Records

Criminal history records range between two extremes. At one pole, practitioners define the criminal history record as what has long been termed the "rap" sheet -- the record of arrests and prosecutions. Most of the nation's criminal history records resemble the minimal rap sheet that satisfies the FBI's reporting requirements.[108] These focus almost exclusively on identifying convicted felons.[109] For national purposes, the rap sheet would be sufficient. Given the present lack of reliable arrest and disposition reporting in most states, even to achieve this minimal level of criminal history records would be an arduous task.

At the other pole, some practitioners suggest that the criminal history record should include far more than arrests and prosecutions. They argue for incorporating victim information, detailed data about the crime, and information about the offender and the justice process. Extended to its logical extreme, this type of criminal history record would resemble an Offender-Based Tracking System (OBTS). The record would contain virtually all information about the offender from the initial incident through final

[107] Immigration Act of 1990. A bill of technical amendments to the Immigration and Nationality Act enacted on December 12, 1991, amended section 503 of the Omnibus Crime Control and Safe Streets Act of 1968 to change INS reporting requirements for convicted aliens. Enacted as PL 102-2323.

[108] FBI Recommended Voluntary Standards for Improving the Quality of Criminal History Record Information (56 Fed. Reg. 5849 (1991)).

[109] To improve the identification of felony offenders, states can use the FBI Interstate Identification Index (III). The III will rely on the FBI's Integrated Automated Fingerprint Identification System (IAFIS), which in turn will rely on each state's ability to support criminal history records with fingerprint identification (Voluntary Standard #3 calls for each serious offense to be supported by fingerprints). See Chapter II for more information about the IAFIS.

release from the justice system, reflecting the complete case files of law enforcement, prosecution, the courts and corrections.

Neither pole is practical or achievable. Maintaining criminal history only as a limited rap sheet, even with charge tracking added, would continue to frustrate the contributing and using agencies to such an extent that cooperation would become questionable. Viewing the criminal history record as the single source of all information about the offender creates an enormous administrative and reporting burden for each agency, along with unmanageable costs. The state must seek a middle ground for a criminal history repository.

The key to attaining the middle ground for Alaska's repository is to have the users of the repository define the data elements needed. Designers of the repository need also to insure that the records comply with federal initiatives such as the Brady Bill, the Child Protection Act, and notification to the Immigration and Naturalization Service of convicted aliens. The statistical communities in state and federal offices also must assure that the repository contains the data needed to understand the justice process.

C. Elements of a Criminal Case History (CCH) System

This section describes the CCH repository recommended for Alaska. The CCH must contain methods of identifying each person as a unique individual and each event as a unique occurrence. The information must be supported by fingerprint verification. The repository itself will not contain all of the data, but will include a series of status flags and pointers for each offender. Overall, the repository will offer services including offender indices that list all offenders of a certain type, victim notification, and job applicant checks to verify that applicants do not have certain types of convictions or records. The repository structure must insure the information is reported electronically to the greatest extent possible to reduce the chances of error in transmission, as well as to assure timeliness. Other methods of insuring accuracy and completeness will include disposition monitoring, validation criteria, and edit checks. Other technologies, particularly bar coding and document scanning or OCR, could enhance the usefulness of the repository. Finally, the CCH must interface with other data repositories in the state, and in other jurisdictions. It should meet standards set nationwide for these interfaces.

1. Offender and Event Tracking

Offender and event tracking includes all of the techniques and data elements needed to insure that the information contained is accurate and adequate.

a) Identifying Numbers

Each offender must be identified by a unique number. In Alaska, agencies have agreed that the offender number will be what is now termed the "ID/LIC."[110] Separately, each arrest must have an identifying number. State agencies agreed in 1990 to use an Arrest Tracking Number (ATN). Within the event, each charge made against the offender, whether noted by law enforcement or filed by the prosecutor in court, or created in any other way, must be recorded and its disposition accurately noted. Although each criminal justice agency now tracks charges, the agencies have not agreed on a uniform system of tracking charges from their creation through to their final disposition.

ATN -- The ATN permits the state to track each criminal incident brought into the justice system from its beginning through the final disposition, and allows the information about the incident to be transferred among agencies completely automatically. The ATN starts with the case, at a time when accurate identification of the person involved often cannot be guaranteed. Until law enforcement, corrections, or court personnel fingerprint the defendant, the ATN serves to tie together the case management numbers assigned to the event by the individual justice agencies' case management systems. The recently designed system of stick-on labels with the ATN imprinted, to put on fingerprint cards, will help assure that the ATN stays with the correct defendant. The state may have made a cost-based decision not to print the fingerprint card as the first part of the incident tracking form.[111] We recommend that the state reconsider this possibility. The state already has added a check digit to the

[110] This is the Alaska driver's license number or a state ID number. It is not a driver's license number issued by any other state.

[111] The Criminal Case Intake and Disposition Form (CCID) has the ATN printed on it. Law enforcement and state prosecutors use the CCID to track basic information about the offense, arrest and prosecution.

ATN to help improve its integrity, and should consider bar-coding, which would eliminate manual data entry and greatly reduce errors in transmitting the ATN.

Person ID Number and Fingerprint Support -- Every defendant must have a unique number for identification. The ATN does not suffice because criminal justice agencies must be able to review every offense associated with the unique individual. As noted, the agencies have agreed, in concept, to use the ID/LIC number in a criminal history repository.

The ID/LIC may not be available at the time of arrest, or may not be fingerprint-verified until some later time in the criminal justice process. Several national groups[112] have defined positive identification of an individual as identification by comparing fingerprints.[113] In most states, including Alaska, an identification number supported by fingerprints does not reach the CCH until weeks or months after an arrest. Meanwhile, the offenders and their cases proceed through the justice system. If all of the information is connected by the ATN, the CCH can match the offender to the event reliably.

Positive identification helps to maintain system integrity and enables efficient automated transfers of data. Fingerprint verification assures that the ID/LIC belongs to a single individual, and that the state always can distinguish that individual from every other individual.[114] The CCH can combine the ID/LIC, the fingerprint verification, and other matching data (e.g., date of birth, name, race) to confirm the association of individuals and events. The automated matching greatly reduces the need for redundant manual entry of data, and transforms the ways that agencies contribute to the CCH. We

[112] Groups include the FBI, SEARCH Group Inc., and the National Consortium for Justice Information and Statistics.

[113] The first FBI Recommended Voluntary Standard states: "Every state shall maintain fingerprint impressions or copies thereof as the basic source document for each arrest (including incidents based upon a summons issued in lieu of an arrest warrant) recorded in the criminal history record system."

[114] Obtaining the fingerprints brings up many other issues about the technology used for prints, who should take them, and so forth. We will not go into these issues, except to note that Alaska's fingerprint system does not at present produce fingerprint images that comply with the NIST standards (National Institute for Standards and Technology). The state should plan to comply with the NIST standard in time for the implementation of NCIC 2000 and the FBI IAFIS. Alaska would have to expend a considerable amount of money to enable the current AAFIS system to comply with the NIST standards.

recommend that the state adopt the pending legislation[115] that requires fingerprinting of most offenders.

b) Demographic Information

Demographic information includes personal identifying characteristics such as name, date of birth, race/ethnicity, gender, height, weight, hair color, and numbers such as social security number and FBI number, as well as the ID/LIC. The state should capture as much of this as possible at the time of arrest. Agencies can transfer the information as needed to their own data bases using automated routines, and can validate information in their own files using the demographic characteristics for matching purposes.[116]

c) Event Information

We recommend that the state use the Eighteen Elements for the criminal history that SEARCH defined as the starting point for determining the types of event information to include in the CCH. These represent a generic model that the state's criminal justice agencies have begun to review and apply specifically to Alaska's needs. The Eighteen Elements include incident data prior to the arrest, as well as more information about the offender and the justice process than is now included in the criminal history records. The next chapter describes the specific pieces of information that we recommend the CCH should include about each event and offender. Some of the information (e.g., detailed probation and parole information) may actually reside in another agency's data base, with the CCH using a "pointer" to indicate where the user should go to find the complete data.

[115] See Appendix C for more detailed comments on the legislation.

[116] For example, the state can initiate an automated name search by using the key numbers - ID/LIC, Social Security, and FBI. If they match exactly, the system can call on the other demographic variables to validate the match. Then the system can automatically send the ID/LIC to the AFIS fingerprint digital image retrieval system to download the fingerprint image for verification. The verification process can select several candidates that meet some of the demographic validation criteria and compare their fingerprint images in much less time than a manual search on a single candidate would take. Automated name searches that do not result in a hit or that cannot be automatically validated would go to a queue for problem resolution. If manual name searching does not make a match, the operator could send the fingerprint card to AFIS for a technical search.

d) Charge tracking

Many arrests lead to multiple police charges. Prosecutors and courts may modify these charges at different points in the process, by declining to prosecute some, reducing or changing others, or adding new charges. Central repositories routinely receive court dispositions that do not match the charges initially reported by the police or prosecutor. The ATN tracks information to a particular case, but the disposition of charges within the case remains ambiguous.

The correct association between a charge and its disposition is critical because many statutes rely for their effect upon conviction of a specific offense. If the prosecutor drops a charge, substitutes another, or the defendant is acquitted, the consequences for the defendant and many other persons differ greatly from those imposed if the defendant was convicted of the original charge. Law enforcement officials, for example, have commented that they need to know that the original charge in a domestic dispute indicated a violent offender, even if the charges were dismissed during the prosecution of the case. Prosecutors and judges also said that they use this information when setting bail and determining sentences. Corrections officials said that they need to track charges to know the final disposition of each charge to ensure that the offender serves the appropriate time for each offense.

Charges should be tracked with a unique number for each charge. Perhaps the easiest way to number charges is to attach a unique suffix to the ATN, so that charge #1 becomes ATN+01, and so forth. Alaska's CCID form contains a charge tracking scheme that users are implementing with reasonable success. Subsequent printings of the CCID form should carry the unique charge tracking numbers for all contributing agency segments of the form. All new or modified case management systems for any criminal justice agency should provide mandatory fields for charge tracking. Planners can overcome many of the difficulties of tracking charges in a manual system by careful design for automated systems.

e) Statute-based Offense Records

The CCH should record offenses using the state statute number. The CCH or individual agencies can incorporate translation programs or other means of including UCR codes or other ways of identifying offenses, as needed. Users can distinguish between felonies and misdemeanors for most (but not all) offenses based on the statute number. The CCH can flag certain types of offenders automatically, using the statute number, and can construct indices and statistical analyses more easily.

2. CCH Services

The CCH can offer a variety of services to the criminal justice agencies, including victim notification, status flags, offender indices, and job applicant screening.

a) Status Flags and Offender Indices

Status flags identify particular types of offender. The FBI Recommended Voluntary Reporting Standards for Improving Criminal Record Information call for a flag for each offender convicted of a felony. The new Child Protection Act requires states to maintain a record of and report on specified offenses against children. Indices list all offenders of a certain type, such as all sex offenders. Alaska should examine its own statutes to find existing provisions that mandate the creation and maintenance of lists of specific offenses and offenders.

Using the statute number for each offense as the key, the CCH system can flag each individual offender, and also can create lists that report all offenders of a certain type. The lists can include name of the offender, data about the offense, and any other information that the state believes necessary. Justice agencies, victims, or the general public can review the lists, as appropriate.

b) Victim Notification

Alaska does not fully implement its victim notification law.[117] The state could enhance the CCH to incorporate the information and procedures necessary to notify victims promptly of an offender's status and release. The system would store the victim's name and address in a secure location. Information about the offender's court dates, parole hearings, and release from custody or supervision would come from the planned disposition fields. The system could automate victim notification by setting flags in the CCH that will alert agencies with victim notification responsibilities. The

[117] AS 12.61.010-900, and AS 33.30.013.

system could prepare a form letter which would be reviewed by CCH staff before mailing to the victim, to verify that the notification is both appropriate and accurate.

c) Job Applicant Reports

The system should check the criminal history records for job applicants, and generate a report in much the same way that it handles victim notification. For some types of jobs, e.g., school bus driver, certain types of convictions, e.g., child abuse or molesting, are of critical concern. Other types of employers need to know the applicant's entire conviction history. The CCH can respond with part or all of the record, using status flags and programming to search the applicant's history and prepare a printed report.[118] The automated procedures could save substantial time and money over the present manual searches, and the public would have more accurate records on which to rely.

d) Specialized Reports

The CCH can serve as a rich source of information about the criminal justice system for the legislature, agencies, universities, and the public. Structuring the CCH on a relational data base permits any data element in the data base to be related to any other element. Agencies can review sentencing, probation and parole decisions, recidivism, substance abuse issues, and the relationships among a wide range of variables. Security provisions and user agreements will prevent breaches of confidentiality.

3. Repository Structure

Certain characteristics of the repository's structure will affect its security, its usefulness and its ease of maintenance. These include automated disposition reporting, disposition monitoring, inquiry purpose codes, and audit capabilities.

[118] The system would prompt the operator if dispositions appeared in the record without a statute number. The operator then would search the entire record, and take any other steps necessary to ensure accurate reporting.

a) Automated Arrest and Disposition Reporting

Using the ATN and ID/LIC as the initial keys for tracking and matching event and offender information, agencies can electronically transfer all needed information to the CCH without manual intervention. This will expedite the creation and updating of the criminal record, significantly reduce labor involved in validating data and reconciling arrest and disposition information, and will eliminate redundant data entry with its attendant errors. With correct ATN and ID/LIC numbers used consistently, fingerprints can be linked to the correct individual and offense. Electronic transmission and recording of arrest and disposition information depends on the integrity of the various case management systems. The CCH can perform automated data validation tests before registering case information in the criminal history.

b) Disposition Monitoring

Alaska's CCH should monitor the dispositions reported to ensure that records are complete, accurate and timely. A disposition monitoring system checks the dates of initial arrests and creates a report of missing dispositions after a specified interval. Staff can then review prosecutor's and court's reports to determine the status of the arrest. By routinely and automatically monitoring disposition information, staff can identify problem areas and work with agencies to correct them.

c) Inquiry Purpose Codes

Inquiry purpose codes limit the kinds of inquiries that external agencies can make of the criminal history records. Other inquiry codes record the kinds and numbers of queries the system receives. Brady Bill requirements exemplify one use of inquiry codes. Criminal history record checks for persons wanting to buy firearms will increase the CCH workload significantly. Justice system agencies, the U.S. Congress, and the state legislature all will want to know about this effect of the Brady Bill. If each time a Brady inquiry is made the system codes it as such, the CCH can separate Brady inquiries out to report on the bill's impact.

Alaska justice agencies planning computerized information systems should consider the types of inquiries they will need to make of the CCH, and program them as inquiry purpose codes.

d) Audit Capabilities

Staff should audit data quality in the CCH regularly. The time required for audits in the short run pays back because the overall quality of the data improves. Every incomplete or inaccurate data element that staff must check manually reduces the overall usefulness of the automated CCH. Programmers can build several features, such as mandatory fields for data entry, into the case management systems that supply data to the CCH to reduce errors at the origin. The CCH can apply edit checks and validation criteria to data coming into the system to insure that electronic submissions are accurate and complete. Disposition monitoring and periodic audits of the CCH will highlight other data problems. Staff can work with agencies to improve data entry and submission, rather than spending substantial time tracking down incomplete data piece by piece.

4. Other Helpful Technologies

The state could enhance the effectiveness of the CCH by using new technologies to eliminate manual labor and increase the accuracy of the data stored and transmitted. Bar coding was mentioned in the discussion of the ATN as a method of greatly reducing the time needed to transcribe the ATN number, and as a technique that would greatly reduce the opportunities for errors in recording the number. Document scanning also could reduce errors, perhaps serving as a transition between the present manual systems of disposition reporting and fully automated systems. OCR (Optical Character Recognition) scanners can capture typewritten dispositions as text rather than images, permitting the information to be used directly.

The state also could consider using OCR to read typed fingerprint cards. All demographic and offense data on the card would be read to the CCH, while the system would capture fingerprint images in NIST-compliant format and send them to AFIS for processing. The system can receive electronic arrest reports at present. If combined with scanned fingerprint card information, the system would have many of the key elements needed to automate the process of searching for offenders' names and making positive identifications.

5. Interfaces with Other Systems

Alaska's CCH must provide data to, and receive data from, other parts of its own justice system, and other states' and the federal government's information systems. Various standards, some voluntary, some mandatory, have been set for these transactions. Two of the most important interactions are the AFIS/CCH interface, and participation in the Interstate Identification Index (III).

a) AFIS/CCH Interface

Alaska currently cannot transfer data between its AFIS (fingerprint identification) system and the CCH. The ability to transfer data would speed up the process of identifying defendants, and would allow the state to respond to requests for information more quickly. At a minimum, an interface between the two systems should transfer demographic data to eliminate redundant data entry. Controlling the transfer with the ATN would permit the AFIS to assign ID/LIC numbers following a search, and to transfer the ID/LIC, ATN, and demographic data to the CCH to create a new record.

A more sophisticated interface would integrate the components of the two systems so that a name search hit on CCH could send an ID/LIC number to the AFIS digital image retrieval system, and retrieve the proper image and bring it back to the records division. This makes name search verification a one-step automated process. The present name search verification process requires that the fingerprint card itself, along with the potential name and ID/LIC be sent to AFIS to retrieve the image. Then the information must be sent back to the CCH. Because the state has a limited number of AFIS verification terminals, staff often perform the verification process manually. Given the age of the current AFIS system, building an AFIS/CCH interface would be expensive and would not be cost-effective. Instead, the system should be replaced.

b) Interstate Identification Index (III)

States participating in the III must provide full criminal history records to justice system agencies, including agencies in other states and the federal government. The Index serves a variety of purposes, including criminal investigations, risk assessment of offenders, bond setting, charging and sentencing decisions, and criminal justice employment. Alaska is a single-source reporting state participating in III through the

Department of Public Safety. DPS has agreed to submit all criterion arrest, court and correctional fingerprint cards and (when possible) the related final disposition reports to the FBI Identification Division until the department is approved to submit only the first arrest card.

Alaska must sign several agreements to participate in the National Fingerprint File (NFF), including the NCIC User Agreement (provides for continued services for authorized criminal justice agencies), and the Interstate Compact (for services related to non-criminal justice uses of criminal history record information). The state also must meet a series of minimum standards for completeness and accuracy of the information in its CCH.[119]

D. Conclusion

The state of Alaska has made great strides in improving the quality and usefulness of its criminal history record. The use of the ATN, the pending legislation for fingerprint records and justice system information, the degree of automation in arrest reporting, and the development of the Troopers' reporting system (CRIMES) all attest to efforts to continually improve criminal records. Many of the data elements and procedures needed for the model CCH already exist or are envisioned in the Department of Public Safety's and other agencies' plans. The proposed CCH builds on what exists to create a repository that can serve the needs of the state as well as local, federal and other state governments.

[119] These standards include: 1) An NFF participant must continue submitting criterion fingerprint cards to the FBI for all records not indexed in III with the state's unique person identifier number (in Alaska, the ID/LIC); 2) An NFF participant must ensure that the person identifier number is on all fingerprint cards not identified at the state level and submitted to the FBI for establishing an NFF record; 3) The participant must submit the second and/or subsequent fingerprint card to the FBI when the original fingerprint card established an incomplete fingerprint classification, or contains a new amputation or permanent scar; 4) The participant must send an electronic message to the FBI when the second and/or subsequent criminal fingerprint card is identified with an NFF record; 5) The participant must add supplemental identifiers to NFF records maintained by the FBI when a second and/or subsequent criminal fingerprint card is identified by the state and contains identifiers not previously recorded; 6) An NFF participant must search both criminal and fingerprint cards prior to their submission to the FBI; and 7) A participant must provide its record for all authorized purposes.

Chapter VI

Criminal History Record Data Elements

In this chapter, we discuss the specific data elements that a criminal history repository should have.

A. Introduction

This chapter of the strategic plan lists the data elements recommended for the Alaska Criminal History Record. The data elements were developed to meet the needs of the Alaska criminal justice community, as well as to comply with interstate and federal initiatives in criminal justice. Collectively, the data elements support integrated criminal justice information system in Alaska, providing the users of the criminal history record with timely information about offenders and their contacts with the justice system.

In an integrated, multi-agency systems environment, the recommended data elements will enhance the utility and functionality of the criminal history record. Instead of a static "flat file" of arrests and dispositions, contributing agencies will build a dynamic criminal history record through the electronic transmission of data. Accordingly, the criminal history record should represent a sub-set of the case management systems of law enforcement, prosecution, courts, and corrections. When a contributing agency enters or updates data, the automated system will electronically download data elements to the criminal history record. Any changes in the status of an offender's case in the systems of the contributing agencies will cause the criminal history record to be updated.

Because agencies will transfer data elements electronically, the larger number of data elements in the record will not burden staff with manual data entry. Moreover, contributing agencies will not be burdened with numerous manual reporting tasks to update the criminal history record. Key numbers, such as the Arrest Tracking Number (ATN), will facilitate electronic transfer while automated data-validation routines will help preserve data integrity. The Department of Public Safety (DPS) should employ routine audits and data quality monitoring techniques to assure the integrity of the data in the criminal history records.

Through unique tracking numbers, case numbers, and status flags and messages, the criminal history record will act as a pointer system to other data bases of information about the offender. Depending on the technical architecture utilized for the criminal history record, the information in other data bases could be obtained through special inquiry commands in the criminal history application. This ability to point to and obtain additional information about an offender depends upon linking key numbers among the contributing agencies.

The criminal history record data elements in this chapter will satisfy the majority of inquiries by users. The elements represent an effort to expand the amount of information in the criminal history record, while not letting the record become so large that it compromises the ability to accommodate the vast numbers of inquiries and transmission of the records via state and national telecommunications systems.

The data elements recommended here should come from the automated case management systems of contributing agencies. The increased number of data elements requires that agencies build and update the criminal history record electronically, as the data sources become available. Some of the data elements listed here may be future goals rather than elements that the systems would add immediately. The ideal criminal history record requires more data than agencies can enter using only manual systems.

National programs are defining the data elements of the criminal history record for interstate exchange purposes through the FBI Interstate Identification Index (III). As part of the effort to define Alaska's data elements, we met with the SEARCH Group to discuss issues identified and progress made by a national task force on the criminal history record. While the SEARCH Group would not release its recommended data elements until the task force complete its report, SEARCH's senior council of the Information Law and Policy Program carefully reviewed the data elements proposed for Alaska and stated that they were consistent with the direction of the task force.

The Alaska data elements proposed here may include more information than those that eventually emerge from the national task force, the FBI III program, and the Advisory Policy Board of the FBI. The Alaska data elements serve the unique needs of the Alaska criminal justice community, while the data elements for III exchange purposes may represent a more limited set for interstate needs. Whatever the task force recommends for III exchange purposes, should be easy for the state of Alaska to provide.

B. Criminal History Data Elements

The criminal history record data elements are presented here, followed by a section-by-section commentary.

1. Flags and Messages

Interstate Identification Index (III) Flag
Single-state/Multi-state Flag
Felony Flag (F,M,V)
Sex Offender
Habitual Offender
Illegal Alien
Mental Defective/Committed to Mental Institution
Unlawful User/Addicted to Controlled Substance
Dishonorable Discharge Armed Services
Renounced Citizenship
Caution(s): (e.g., Violent, Armed and Dangerous, Known Drug Offender, Firearms User Arson)
Total Number of Arrests
Total number of Convictions
Date of Last Arrest

2. Identification Segment

- **Personal Descriptors**

Name (Last, first, middle, suffix)
Alias (Multiples)
Address (Updated)
Sex
Race
Date of Birth
Place of Birth
Country of Citizenship
Height
Weight (Updated)
Hair Color
Eye Color
Scars, Marks, Tattoos, Amputations
Occupation (Updated)
Employer (Updated)
DNA Profile Available (Location)

Palm Print Available (Location)
Photo Available (Location)

- **Key ID Numbers**

State Identification Number (SID)(ID/LIC)
Social Security Number (Multiples)
FBI Number
Department of Corrections Number (DOC)
Miscellaneous Number(s)

- **Record Type**

Criminal
Applicant
Warrant
Juvenile as Adult

3. *Arrest Segment*

- **Agency-Specific Information**

Incident Number (If Available)
Arrest Tracking Number (ATN)
Arresting Agency Name
Arresting Agency Number (ORI)
Arresting Agency Case Number (OCA)
Arresting Agency Unique Person Identifier

- **Arrest Information**

Date of Arrest
Date of Offense
Place of Arrest
Name at Arrest (Last, first, middle, suffix)
Juvenile as Adult Indicator
Fingerprint-Supported Indicator
Arrest Charges:
  Unique Charge Numbers (01,02,03, etc.)
  Charge Counts
  Statute Citation
  Offense Literal Description
  NCIC Offense Code
  Felony/Misdemeanor Charge Indicator

Release after arrest without filing charges
Release Date
Final Disposition

4. *Pre-Trial Status Information*

Bail Denied (Court Name, Date)
Custody in Default of Bail (Court Name, Date)
Bail Set (Court Name, Amount, Date)
Release Type (Bail, ROR, etc.)
Release Date

5. *Prosecutor Segment*

Arrest Tracking Number (ATN)
State Identification Number (SID) (If available)
Arresting Agency Case Number (OCA)
Prosecutor Agency Name
Prosecutor Agency Number (ORI)
Prosecutor Case Number
Prosecutor Disposition:
- Unique Charge Numbers (01,02,03, etc.)
- Charge Counts
- Statute Citation
- Offense Literal Description
- NCIC Offense Code
- Felony/Misdemeanor Charge Indicator

Disposition Date
Filing Date of Information or Indictment

6. *Court Segment*

Arrest Tracking Number (ATN)
State Identification Number (SID) (If available)
Prosecutor Case Number (OCA)
Court Name
Court Number (ORI)
Court Case Number
Court Docket Number
Court Disposition:
- Unique Charge Numbers (01,02,03, etc.)
- Charge Counts
- Statute Citation
- Offense Literal Description
- NCIC Offense Code

  Felony/Misdemeanor Charge Indicator
Disposition Date
Acquittal Disposition Date
Sentence Date
Sentence Length
Term Suspended
Probation
Probation Conditions
Probation Expiration Date
Fine Amount/Restitution
Fine/Restitution Amount Suspended
Failure to Pay Fine/Restitution
Presumptive Indicator
Special Conditions
Concurrent/Consecutive Flag
Bail/Commitment Pending Sentencing/Appeal (Date)
SIS Flag

7. *Appellate Phase*

Arrest Tracking Number (ATN)
State Identification Number (SID) (If available)
Original Prosecutor Case Number
Original Court Case Number
New Prosecutor Case Number
Appellate Court Case Number
Appeal Failed/Waived (Date)
Appeal Period Expired (Date)
Appellate Disposition:
  Unique Charge Numbers (01,02,03, etc.)
  Charge Counts
  Statute Citation
  Offense Literal Description
  NCIC Offense Code
  Felony/Misdemeanor Charge Indicator
Appellate Disposition Date

8. *Corrections Phase*

Arrest Tracking Number (ATN) (If Available)
State Identification Number (SID) (If available)
Corrections/Institution Name (Contract Jail, Prison, Probation and Parole, H&SS)
Corrections Agency Number (ORI)
Corrections Agency Unique Person Number

Court Case Number
Status--Received, Release Pending Trial, Confinement, Parole Violation, Parole Revocation, Deceased, Unconditional Release
Status Date
Last Known/Current Address
Emergency Contact
Escape Date
Return Date

9. Executive Clemency

Agency Name/Official
Action--Pardon, Commutation of Sentence, Restoration of Rights, etc.
Action Date

C. Commentary on Recommended Data Elements

In this section, we discuss the data elements detailed above by major category.

1. Status Flags and Messages

Status flags and messages provide quick access to summary information about an offender. They also respond to national initiatives. The Interstate Identification Index (III) Flag and the Single-state/Multi-state Flag meet the requirements of III participation, while the Felony Flag responds to the FBI Recommended Voluntary Standards for Improving the Quality of Criminal History Record Information. The Sexual Offender and Habitual Offender flags meet state mandates to identify certain classes of offenders. Based on statutes coded in the criminal history record the CCH can set flags automatically. The Illegal Alien Message meets Immigration and Naturalization Service's (INS) mandate to identify illegal aliens convicted of a felony offense.

The Mental Defective/Committed to Mental Institution, Unlawful User/Addicted to Controlled Substance, Dishonorable Discharge Armed Services, Renounced Citizenship messages respond to requirements set in the Brady Bill. Setting messages or flags for the Brady categories depends on having both a source and a delivery mechanism for the information. In some states, for example, legislative rules make information on persons institutionalized available to the central repository. The delivery mechanisms can vary from hard-copy printouts, to magnetic tapes, to on-line electronic transfers.

The Caution Message for Violent, Armed and Dangerous, Known Drug Offender, or Firearms User is a standard message in criminal history records that provides quick alerts for law enforcement dispatchers to inform officers in the field.

The status fields of Total Number of Arrests, Total Number of Convictions, and Date of Last Arrest can provide quick summary information on an offender, automatically generated by the system.

2. Identification Segment

The Identification Segment consists of personal descriptors, key identification numbers, and record type. Several improvements make the data elements more useful than the typical elements found in a CCH. Address, weight, and occupation have "update" requirements, rather than representing the data from the first arrest. Dynamic updates of "address" help locate offenders. The CCH keep a chronological file of all addresses, with last-known address most easily available. "Alias" allows for multiple names to increase the chance of a name-search hit. (A multiple for "date of birth" and "social security number" increases the chances of a name-search hit.) The CCH should include biometric identifiers, such as DNA Profile, Palm Print, and Photo. For these, the CCH provides pointers. For example, the forensic laboratory usually keeps DNA profiles, with access using the SID number.

Key ID numbers are standard elements that help identify the offender and facilitate the name-search function.

Record type is a flag that alerts the user to the types of records that are available. While Alaska does not currently store job applicant records, the CCH should include a field for the data element, for future use.

3. Arrest Segment

The elements also provide "pointers" to the case files in the contributing agencies. For example, the Incident Number notifies users that an incident report exists at the arresting agency, available through the unique incident number) which is "keyed" to the ATN for this arrest event). Other data elements keyed to the event are Arresting Agency Name, ORI, OCA, and Arresting Agency Unique Person Identifier (as distinct from SID).

Depending on the technical architecture chosen by the state, and on whether the incident report is on line at the local agency, the user could access the incident report through the CCH system server.

Data elements that link arrest and disposition information among criminal justice agencies characterize the Arrest Segment, as well as the Prosecutor Segment, Court Segment, Appellate Phase, and Corrections Phase.

Three other elements in this segment, Date of Arrest, Date of Offense, and Place of Arrest, expand the information normally captured by the criminal record. The CCH also includes two indicators of the defendant's record, Fingerprint-Supported Record (shows that this arrest is supported by positive identification), and Juvenile as Adult (flags the age of the offender at the time of this arrest event).

Arrest Charge data elements include charge tracking with unique numbers for each charge (01, 02, 03, etc.). We recommend that the unique charge numbers be a suffix to the ATN. This will let agencies track charges and associated counts through the criminal justice system. The CCH includes an NCIC Offense Code to ease interstate exchange of criminal history records. The NCIC code shows users in other states how Alaska state statutes compare to federal statutes. The Felony/Misdemeanor Charge Indicator ensures that all users of the record know the seriousness of the charge.

Release After Arrest Without Filing Charges indicates the final disposition of the case. This information is necessary to complete the record of arrests and final dispositions.

4. Prosecutor Segment

The Prosecutor Segment includes the ATN and Arresting Agency (OCA) as key links to the Arrest Segment. The SID (Alaska's ID-LIC) should be included, if it is available at this point. Agencies should not assign an ID/LIC to an arrest or prosecution segment until fingerprint comparison supports positive identification. Linking the ID-LIC to the ATN provides a way to electronically transmit the ID-LIC and inform the prosecutor of any aliases for the offender. The ATN acts as a process control number to cross-reference a unique case as it progresses through the criminal justice system.

Because the ATN can be linked to the ID/LIC before the positive identification by fingerprint comparison can take place, it serves as a reliable unique person identifier.

In the Prosecutor Segment, charge tracking should correlate with the Arrest Segment sequence of charges. If the prosecutor modifies a police charge, the same sequence of unique charge numbers should be used to show the charge as modified. If the prosecutor adds a charge, a new unique charge number should be used. A decline to prosecute should be treated as a final disposition and reported to DPS as such.

5. Pre-Trial Status Information

Users of the criminal history record need to know the location of the offender and bail status prior to trial. Statutes in many states, including Alaska (AS 12.30.020(c)(8)), require that judges setting conditions of release shall consider a person's record of prior convictions and appearances at court proceedings.

The CCH needs to keep pre-trial status information current. These data elements should be transferred electronically from automated court management systems.

6. Court Segment

Data elements in the Court Segment facilitate links among the unique case numbers of contributing agencies. The ATN provides the primary linkage, while the Prosecutor Case Number (OCA) links to prosecutor case file information. Charge tracking should maintain the sequence of charges established at arrest and continued through the prosecutor segment. If the court modifies a prosecutor charge, it should use the same sequence of unique charge numbers to show the charge as modified. If the court adds a charge, it should use a new unique charge number.

7. Appellate Segment

The Appellate Segment essentially updates the criminal history record during the appeal process, and records the final disposition according to the same sequence of charge tracking used by law enforcement, prosecution, and courts. It is critical that the ATN be used as key linkage.

8. Corrections Segment

If the courts provide the ATN to the Department of Corrections as part of the offender's commitment order, DOC can use the ATN to ease the name search and positive identification. The new fingerprint legislation provides for fingerprinting at the time of incarceration, adding that DOC must compare fingerprints for positive identification. This provision will allow DOC to use the ID-LIC as a reliable unique person identifier in its case management system. DPS transfers the ID-LIC electronically with data integrity safeguards, then the DOC can transmit correctional disposition information electronically to the criminal history record.

Access to the criminal history record by ATN also will allow DOC to get current court information, such as sentencing conditions and appellate decisions.

The Corrections Segment also calls for keeping the criminal history record current with offenders' last-known address after their release from custody, as well as an emergency contact name and address.

9. Executive Clemency

Executive Clemency includes the other means by which a final disposition occurs, such as pardons and sentence commutations. The courts or corrections system may send the information electronically to the CCH. The actual disposition and authority altering the sentence should appear in the CCH, along with the date of the change and charges affected.

Chapter VII

Alternative System Configurations

The State of Alaska legislature and the criminal justice agencies have agreed that the computerized information systems used to track criminal records and activity need to be more integrated. The amount of integration could range from little more than the exchange of paper documents that occurs at present, to a fully integrated system in which all agencies use the same computer software to manage cases. We recommend looking at a series of intermediate possibilities, with the state relying on independent systems for each agency, a central data repository for criminal history records, and varying levels of access to agency records for other criminal justice system personnel and the public. This chapter examines trends in technology that have helped to shape our recommendations, technical standards that any new systems should meet, criteria to help in the choice of new systems, the range of alternatives that Alaska should consider, and the system that we recommend.

A. Trends In Technology

The past thirty years have seen dramatic changes in computer technology. Many users have moved from the 1960s environment of a single-machine system in which each company's computers operated in a unique style, to the 1990s environment in which many users work on open systems, using a variety of computers, software, networks, printers and peripherals. In the 1960s, people did not expect that their computers would communicate; in the 1990s, people expect that despite radically different structures and capabilities, all of their computers will talk to each other and to everyone else's computers. This expectation is not met, for the most part, in Alaska's criminal justice system. Although agency staff and management can see clearly the benefits of keeping and sharing certain types of data, in reality the agencies' computers and applications cannot interoperate easily. As a result, departments waste time and money duplicating information other departments have, public safety is threatened, and the public and the legislature suffer from the paucity of useful data.

The system alternatives recommended for Alaska all take into account the fact that the state owns a mixture of mainframes and client/servers with networks, as well as stand-alone personal computer systems. To provide a context for our recommendations, we first discuss below the technological trends for each of these components.

1. Open Systems

During the past few years, no topic has attracted as much interest from computer vendors and end users as "open systems." While advertisements tout the commitment of proprietary systems to open systems, businesses and governments are left to make practical sense out of the extensive and sometimes confusing standards that serve as open systems building blocks. The real challenge of open systems is to build a bridge between proprietary systems and open systems so they can co-exist.

Users and manufacturers hotly debate the definition of open systems. One school of thought defines an open system as a system with a published interface that can be used by other systems to access it. Another defines any non-mainframe system as open. While many disagree about the definition of an open system, few argue about its necessity.

Governments attempting to build the necessary bridges between proprietary and open systems face two challenges: application portability and interoperability. Application portability is the ability to run an application on all systems, whether open or proprietary; interoperability is the ability to share data across heterogeneous data management systems.

Users have turned to open systems because of definite benefits. Agencies can buy the components of open systems for less (often, much less). They take fewer risks in an uncertain market, because of the smaller investment. They can upgrade more easily by adding components as their needs change. Their choices of hardware and software do not lock them in to one system. They can piece together systems from many different sources, and can communicate or share data with many systems running other manufacturer's products.

Open systems have drawbacks as well, that may not be as obvious as the benefits. Users have found that very large data bases may still be difficult or impossible to run on personal computers. Agencies may find that they cannot adequately protect data on open systems, either from day-to-day security problems or from disasters. Open systems may reach a limit in the number of users or operations that the system can support, resulting in degraded performance. Agencies may invest less in training and support for the smaller systems, reasoning that they are less complex, and then find that as much or more training and support are required for open systems as for the mainframe systems. The ability to personalize and customize each component of the open systems, while advantageous, also means that agencies may find maintenance of the systems difficult.

When attempting to establish as open a system as possible, users should pursue technology that:

- Supports all major hardware, operating systems, graphical user interfaces, and networking environments;
- Ensures portability of applications across Unix and proprietary systems;
- Adheres to industry standards; and
- Provides interoperability with other vendor software.

2. Client/Server Technology

Client/server technology includes four types of interacting components: 1) one or more clients (usually personal computers); 2) the server (often a high-end personal computer or a mini-computer); 3) one or more data base management systems; and 4) a network that connects everything. Client/server computing distributes the processing work among the server and clients instead of letting it all happen on a single computer. This can allow faster and easier access to the information on the system. Having the computing work done close to the user lets the user gather, store and use information more efficiently. Within limits, more programs, clients and servers can join the network without slowing down the whole system. Because the architecture is simpler, setting up a new application can be easier and less expensive than on a mainframe. A wide range of vendors can supply new parts for the system, reducing cost and the disadvantages of limited sources of supply.

The market is moving towards greater use of client/server technology and away from reliance on mainframes. Even so, client/server technology has not matured to the point that it can fill all needs. Mainframes will remain in some form for the foreseeable future -- often as data repositories and anchors for mixed-vendor networks. The result will be a mixture of mainframes, open servers, and PC LANs.

3. Mainframes

Mainframe vendors recognize that they must compete in terms of cost and flexibility with client/server systems. At present it appears that they may begin to use CMOS chips to compete with RISC-based computers using multiple, parallel processors.[120] Although individual chips and components might fail, the system as a whole could be nearly perfectly reliable. Mainframe software will have to be rewritten to run on the new machines; the interim versions may not be as well-developed as the versions that had been refined over the years for mainframes. Older programs based on COBOL or assembler languages may not translate as easily to the new hardware as applications such as CICS, SQL or DB2 that depend on many layers of system software.

Mainframe vendors are working to solve two problems. First, they must build machines based on small engines that can provide working platforms with the same stability, flexibility and extendibility that mainframes now offer. Second, they must improve price/performance ratios equivalent to the various alternatives. One pricing problem is that current licensing structures for software would put purchasers of the new machines at a disadvantage. Another is that customers may have to maintain their existing mainframe systems during a transition to newer systems.

4. Telecommunications

Networks tying together computers of different sizes, types, and abilities have proliferated during the past ten years. They range in scale from office networks that connect a handful of personal computers together, to large-scale networks that serve many smaller intra-office networks within the same department or company, to wide area networks (WANs) that pull together networks and computers in completely different locations or even organizations. The networks use various devices, including

[120] Mainframe vendors, particularly IBM, understand they may need to drop prices significantly. Large information-processing engines are inappropriately expensive to build and maintain. The small engine epitomized in the single-chip microprocessor is the least costly source of computational power. The aggregate power of a single system (i.e., a CMOS-based parallel transaction and query set of highly coordinated computers), could increase in an almost unlimited fashion to compete in cost against other platforms, such as Unix machines and the AS/400 mid-range line.

bridges, routers, and internet nodal processors. Like the other components of client/server combinations, components typically come from different vendors. This marks a radical shift from the situation ten or fifteen years ago when the purchase of a computer dictated the purchase of a certain type of network.

Most organizations are moving to open systems in which smaller networks (local area networks, or LANs) are joined through routers that support a wide variety of equipment and programs. This trend toward increased sophistication in handling many different protocols (or ways of solving a given problem) will continue because it eases an organization's move towards completely open systems. The multi-protocol routers let departments develop open systems alongside existing proprietary systems, saving the investment in the proprietary system and reducing the risks of relying entirely on the newer system.

IBM's SNA protocol, on which Alaska's state government mainframes are built, is the last major system to move towards compatibility. The Department of Administration has developed a plan to upgrade the existing SNA network to a multi-protocol backbone within the next three years. Integration of the criminal justice agencies' information systems depends heavily on DOA's success in achieving this goal. Unfortunately, the Department of Administrations's communications backbone proposal was not included in the Governor's proposed capital budget this year. However, the Department still plans to implement at least part of the upgrade.

5. Evolving Technologies

The reader must recognize that, while we refer to Unix, Oracle, and related tool sets throughout this document when referring to open systems and the newer technologies, we do not intend to imply that Unix is the only "open" operating system, or are Oracle and the tool sets discussed in this document the only "open system" software tools available. In fact, products mature and vendors develop new offerings so rapidly that agencies should select the right development and operating software when they are ready to develop or implement the new systems.

This chapter details various hardware and software technologies and related costs. Users must compare the costs of each alternative, but should keep in mind the fact that newer technologies have significant benefits that may offset some increased cost.

Agencies will have easier access to the information stored in their computer systems, and will be able to use it to manage caseloads and work far more effectively.

B. Setting Standards

To successfully integrate the criminal justice information systems the state must create and adopt standards for using and sharing the information. We believe the Division of Information Services, working through the Telecommunications Information Council, should chair a group of criminal justice users in developing open systems and client/server standards. The list of standards we proposed is not all inclusive; but it is a starting point for addressing "open systems for information access and sharing." In other words, these standards are an important component of a successful distributed system implementation. We set the proposed standards out in detail in Appendix D.

In this report, we describe the basic data elements we believe should reside within the criminal history repository. We also recommend that agency systems electronically interface with the repository for data transfer. The format for this transfer and the frequency and method of transfer for each agency need to be defined.

The actual format for the transfer should be standardized to be consistent across agency systems, recognizing that not every agency will transmit every data element. The method of transfer, on-line versus batch, as well as frequency, may vary by agency, although generally, we believe that on-line processing best serves the needs of the criminal justice community.[121]

C. Technical Evaluation Criteria

As the criminal justice agencies pursue system re-engineering efforts, selecting a data base facility and considering client/server technology versus mainframe systems, the agencies must rank their evaluation criteria in priority order and apply them to the technologies to determine which solution best meets their needs. In the next section, we discuss each alternative in the context of the following criteria.

[121] For example, daily batch downloads of court dispositions may fully satisfy agency users. Real-time online processing might better serve those who need to know the actual physical location of an offender.

1. Ability to Meet Basic System Requirements

Each technical alternative must meet the fundamental requirements defined for a system. Obviously, each technical alternative must fulfill this criterion in order to be considered for system implementation.

Some of the requirements related to this criterion include:

- The ability to use CCH data for statistical and analytical purposes.
- Automatic interface of AFIS to CCH.
- Capture of all arrests.
- Capture of all convictions.
- Merger and consolidation of charges.
- Expungement capabilities for merged and consolidated charges.
- Capture of complete information.
- Additional data elements.
- Interfaces to other systems.
- Facilities to provide for data-quality audits.
- Minimal data entry.
- Easy access to data.
- Increased amount of charge data.
- Participation in III/NFF.
- Continuous system availability.

2. Ease of Use

The CCH repository must be easy to use. System navigation, data entry, inquiries, reporting, and general operation should be straightforward, clear, and easy to understand.

Requirements related to the CCH repository could include:

- An automatic interface to AFIS.
- Automatic interfaces to agency systems.
- Minimal duplicate data entry.
- Keystroke minimization.
- Multiple search criteria.
- Very flexible search and query options.
- Simple-to-use ad hoc query and reporting.
- Must be menu driven.
- On-line help and documentation.

3. *Ad Hoc Data Access*

The repository must quickly and easily generate ad hoc queries and reports of data. Ad hoc access should allow authorized users to obtain any information desired in a wide variety of user-selectable/definable formats. Ad hoc data access also will ensure that programmers can respond quickly to user requests for specific reports and information.

Examples of possible requirements for a CCH repository include:

- The ability to use CCH data for statistical and analytical purposes.
- Keystroke minimization.
- Numerous enhancements for queries.
- Very flexible search and query options.
- Simple-to-use ad hoc query and reporting.
- Facility to extract and download data to end-user computers.
- Ability to save and re-use often-used ad hoc reports and queries.

4. Security

A CCH repository must be completely secure, with access to the system and its data controllable at all levels. Security must be provided at the system, function, data base, data table, and table row/column levels.

5. Ability to Interface with Other Systems

The CCH repository eventually will link into several criminal justice systems that DPS does not control directly. The fundamental premise of the CCH repository is that it will exchange data with--and maintain data from--the other criminal justice systems involved in the justice process. The CCH also must tie into federally controlled applications such as NCIC, IAFIS, III/NFF, and others. This will allow the respective systems to fulfill their missions by maintaining current, complete information.

Specific requirements related to interfaces could include:

- An automatic interface to AFIS.
- Automatic interfaces to agency systems.
- Minimal duplicate data entry.
- Timely access to data by all user agencies.
- Facilitate data-quality audits.
- Hardware independence.

6. Ability to Incorporate Future Technologies

The state of Alaska data processing professionals understand that the fundamental paradigm for computer technologies is shifting and that today's legacy systems are not necessarily appropriate models for future system. The state will develop systems over the next several years that Alaska will use for a significant period of time after procuring or creating them. The systems' designs must incorporate the emerging concepts to ensure that they adequately meet user needs and expectations for years to come.

Specifically related requirements may include:

- Numerous enhancements for queries.
- Very flexible search and query options.
- Hardware independence.
- Facilitate transmission speed while minimizing costs.

7. Integration with the Desktop Environment

The change in the desktop environment from "dumb" terminal devices--such as 3270 terminals--to intelligent workstations--such as PC's--provides a new set of technologies that can be applied to the querying, manipulation, and display of data. Advanced data base, spreadsheet, and document processing tools that run on PC workstations could allow users to make expanded use of the repository information, within the limits of required security.

Specifically related requirements might include:

- The ability to use CCH data for statistical and analytical purposes.
- Minimal duplicate data entry.
- Facility to extract and download data to end-user computers.
- Seamless transitions between application systems.

8. Ease of Administrative Operation

The "Ease-of-Administrative-Operation" criterion represents the ease of controlling and maintaining the day-to-day operation of the CCH repository on agency systems.

Specifically related requirements might include:

- Ease of program maintenance and development.
- Ease of security maintenance.

9. Availability of Skilled Technical Personnel

This criterion represents the likelihood that the state can employ appropriately skilled technical personnel to maintain and service the new systems. If data processing personnel use emerging technologies to develop new systems, the state must train existing personnel in the skills necessary to support the system.

10. Cost

The "Cost" criterion represents the dollars required to design, develop, and implement the new systems. Any cost comparison of mainframe options compared to distributed systems must consider all costs of each system, including performance issues, training and support costs, personnel requirements, and communications.

11. Ease of Migration from the Current Environment

The "Ease of Migration from the Current Environment" criterion indicates the level of difficulty involved in moving, for example, the CCH repository from the existing to a new computer environment.

12. Standards Compliant

As the trend toward "open" systems continues, the computer industry is developing more standards to ensure that systems from different manufacturers will work together in predictable ways. The "Standards-Compliant" criterion represents the importance of standards when making use of the emerging technologies.

Specifically related requirements could include:

- Hardware independence.
- Facilitate transmission speed while minimizing cost.

13. Level of Technical Risk

The "Level-of-Technical-Risk" criterion represents the avoidance of technical risk in designing and developing new applications.

D. Alternatives

In our review of the requirements for an integrated criminal history repository as discussed in this document, we identified several possible technological alternatives for the hardware and software environment that could support agency systems and the criminal history repository. These alternatives involved a variety of technologies, spanning the spectrum of computer, network, operating system, and data base platforms. We carefully reviewed each alternative's merits and problems, and picked out three basic alternatives for further discussion. We describe each alternative below, providing a system schematic, costs, and a discussion of the evaluation criteria. This section focuses on the technology alternatives for the repository and the related agency systems. In the next section, we discuss the recommended alternative, and the recommended direction for application software. We do not present alternatives for application software in this section because we support an approach to this software that incorporates the following, whenever possible:

- On-line interfaces are preferable to batch. These interfaces can transfer information on a regular basis, during off-hours when the updating will not affect on-line inquiries and updating.

- These interfaces should be two-way, whenever possible, to reduce errors and minimize data entry.

- Agency systems and the repository should have the greatest connectivity possible, allowing the DPS system to route queries to the appropriate criminal justice agency when the information needed not stored in the criminal history repository.

1. *Alternative 1 — Continued Implementation on the Existing AMDAHL Mainframes Using ADABAS as the Data Base Management System*

This alternative (shown as Figure 12 on the following page) continues to use the existing AMDAHL mainframes for current and future applications for all agencies except the courts. The state would connect users through its backbone network, which it should upgrade to provide multi-protocol capabilities. Agencies could access the repository via PC workstations, dumb terminals connected to existing agency systems, or, in either case, directly into the criminal history repository.

a. *Technical Considerations*

- **Computer hardware**--The state would not need any new computer hardware, other than possibly new PC's, for this alternative. The host computer would be the existing AMDAHL that supports the current APSIN system.

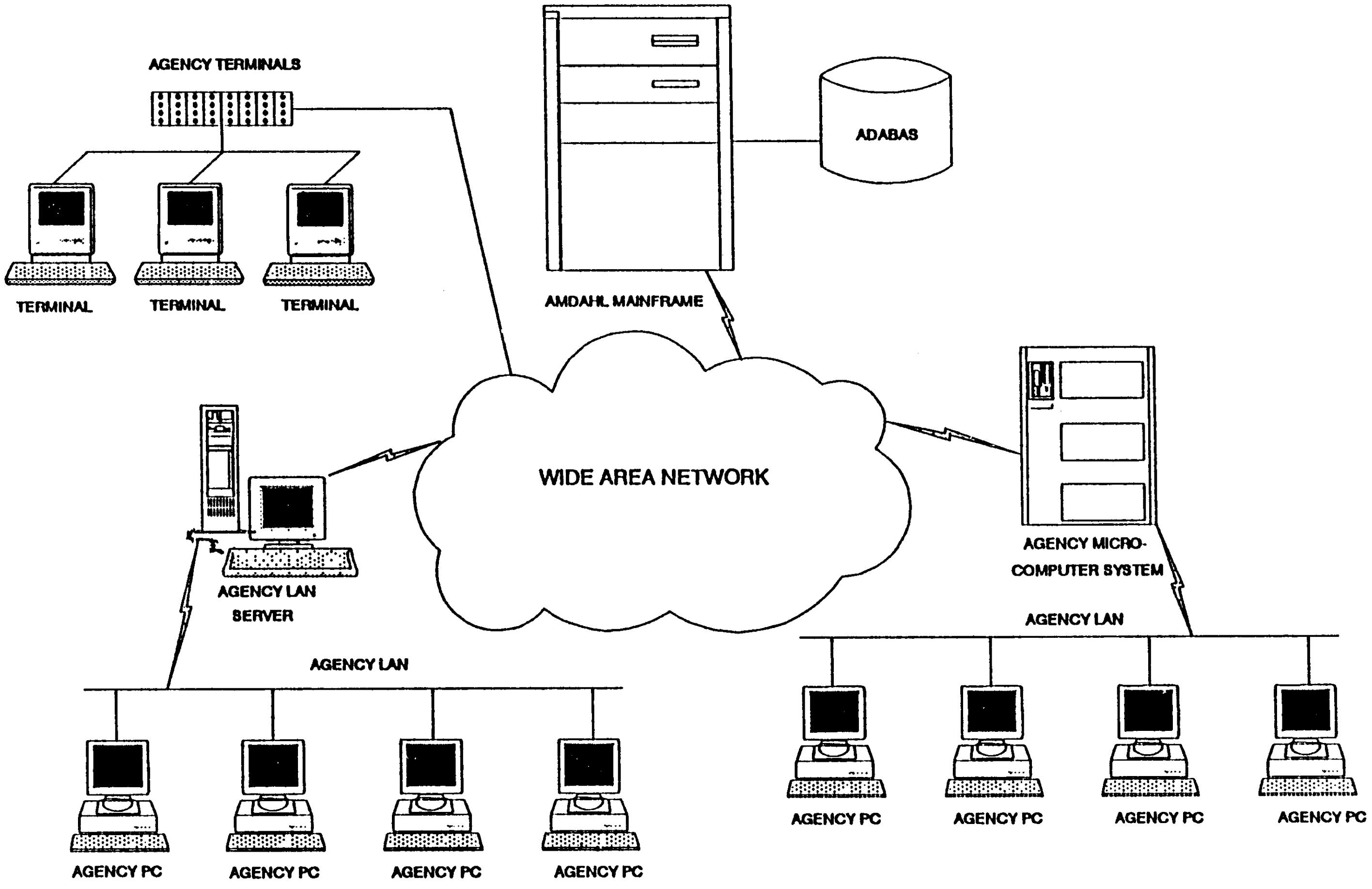
- **Network**--This alternative would not need new network connections. Agencies would access the statewide systems via the same connections by which they access the existing APSIN system.

- **Operating system and utilities**--This alternative uses the existing MVS/CICS configuration running on the state's mainframes for its operating system. The state may need new utilities to connect existing mail systems running on agency platforms until the multi-protocol backbone is in place.

- **Data base**--This alternative continues to use ADABAS as the data base management system. ADABAS can provide the easy, direct access to data—subject to appropriate security—that users have identified as important for enhancing the criminal history repository.

FIGURE 12

ALTERNATIVE 1
EXISTING MAINFRAME
WITH ADABAS



- **Applications environment**--Agencies would continue to develop new applications using ADABAS, NATURAL, and the mainframe. This would perpetuate the same "legacy" systems environment currently in place and would make any later move to distributed or client/server technology that much more difficult.

- **Cost components specific to this alternative**--For this alternative, the departments of Public Safety, Law, and Corrections would continue to use the mainframe and associated software tools for their applications and the Alaska Court System would continue to pursue its system redevelopment efforts, using its existing client/server hardware, Unix operating system, and relational data base software.

  For our one-time and recurring cost estimates related to this alternative, we have assumed that the departments of Law and Corrections will need replacement systems. We estimate that rate-based service charges from DOA/DIS for multi-protocol communications and mainframe services would increase at the rates reflected in our projections. Finally, we project growth in data processing personnel to support new systems requirements under this scenario. This growth would include new staff in DOL (or within DPS to support a new DOL system). The data processing staff of DPS will need more staff to support new in-house-developed applications. The costs for DOA/DIS incorporate the funds needed for a multi-protocol network.

  Tables 1 through 5 following this page detail our cost estimates for this alternative for each agency. The total cost would come to $13,655,000 for one-time costs, and $3,873,000 for 5-year recurring costs, or $17,428,000 total. The high recurring costs would continue indefinitely because of the nature of this alternative.

  DOA/DIS--The one-time costs to implement a multi-protocol network over three years total $3,250,000.

TABLE 1

ALTERNATIVE 1
DEPARTMENT OF ADMINISTRATION, DIVISION OF INFORMATION SYSTEMS
($000)

PROJECT TASKS	FY 95		FY 96		FY 97		FY 98		FY 99	
	Recurring	One-Time	Recurring	One-Time	Recurring	One-Time	Recurring	One-Time	Recurring	One-Time
1. Acquire Hardware and Software and Install a Multi-protocol Network										
a. Statewide E-mail		300								
b. Network Management		160								
c. Statewide Internet		1,953		538.2		298.8				
TOTALS		2,413		538.2		298.8				

TABLE 2

**ALTERNATIVE 1
DEPARTMENT OF PUBLIC SAFETY
($000)**

PROJECT TASKS	FY 95		FY 96		FY 97		FY 98		FY 99	
	Recurring	One-Time	Recurring	One-Time	Recurring	One-Time	Recurring	One-Time	Recurring	One-Time
1. Criminal History Enhancement/Interfaces				600		500				
2. NCIC-2000										
a. Analysis and Design		225								
b. Implementation				500						
3. AFIS Replacement		500		500		500		500		
4. AFIS Live-Scan Devices (13)				487.5		487.5				
5. APSIN/AAFIS/NCIC Integration						250				
6. Network Enhancements		500		115		115				
7. DOA/DIS Rate-Based Service Charges										
a. Network										
b. Mainframe			200		300		300		400	
8. New Staff Resources (3 FTE's)			104		156		164		172	
TOTALS		1,225	304	2,202.5	456	1,852.5	464	500	572	

TABLE 3

ALTERNATIVE 1
ALASKA COURT SYSTEM
($000)

PROJECT TASKS	FY 95		FY 96		FY 97		FY 98		FY 99	
	Recurring	One-Time	Recurring	One-Time	Recurring	One-Time	Recurring	One-Time	Recurring	One-Time
1. Trial Court System Development Cost[1]		<200>		<225>						
2. Appellate Court System Development Cost						125		125		
TOTALS						125		125		

[1] This cost has already been appropriated.

TABLE 4

ALTERNATIVE 1
ALASKA COURT SYSTEM
($000)

PROJECT TASKS	FY 95		FY 96		FY 97		FY 98		FY 99	
	Recurring	One-Time	Recurring	One-Time	Recurring	One-Time	Recurring	One-Time	Recurring	One-Time
1. Trial Court System Development Cost[1]		<200>		<225>						
2. Appellate Court System Development Cost						125		125		
TOTALS						125		125		

[1] This cost has already been appropriated.

TABLE 5

ALTERNATIVE 1
DEPARTMENT OF CORRECTIONS
($000)

PROJECT TASKS	FY 95		FY 96		FY 97		FY 98		FY 99	
	Recurring	One-Time	Recurring	One-Time	Recurring	One-Time	Recurring	One-Time	Recurring	One-Time
1. System Re-engineering		150								
2. Alternatives Evaluation		50								
3. Rapid Prototyping				25						
4. System Acquisition/Implementation				2,000		1,000				
5. Equipment				200		100				
6. Staff Training		25		50		50				
7. DOA/DIS Rate-Based Service Charges										
a. Network			30		50		55		70	
b. Mainframe			180		280		305		380	
TOTALS		225	210	2,275	330	1,150	360		450	

DPS--We extracted the projects related to the criminal history repository from the DPS Information Systems Management Plan. These included criminal history enhancements, NCIC-2000, and AAFIS/APSIN integration. We also included network enhancements, new staff resources required for DPS' new system requirements, and projected increases in DOA/DIS rate-based charges. In addition, we included the costs of acquiring a new AFIS system and thirteen live-scan devices. Three of these live-scan devices are intended for use by DFYS for juvenile fingerprinting. The new one-time charges total $5,780,000 and the new recurring charges total $1,796,000.

DOL--The DOL costs include creating a two-person data processing staff and replacing PROMIS with a new system. Charges for new equipment and increased DOA/DIS charges are included. New one-time charges total $725,000 and new recurring charges total $727,000.

Alaska Court System--The court system intends to use its current hardware and system software for its new systems, use its current staff for system and equipment maintenance and contract with other firms for software development. Thus, the court system's new one-time costs total $250,000. The costs for the trial court systems have already been appropriated.

DOC--The DOC costs include replacing the current OBSCIS system with a new system, acquiring new PC and network equipment, training staff, and paying new DOA/DIS charges. The new one-time charges total $3,650,000 and new recurring charges total $1,350,000.

- **Significant issues**--Since this alternative uses the existing system platform, it does not require any significant new computer systems or networking hardware.

b. Evaluation Criteria Applied to Alternative 1

The following discussion describes how the first alternative complies with each of the technical-alternatives rating criteria.

- **Ability to meet basic system requirements**--This alternative uses the ADABAS data base on the existing state mainframe system. Such an architecture can fully support the basic requirements of the repository. It does, however, limit the choice of computer platforms that the system might run on in the future, as well as limit the tool sets available for developing new applications, and for providing ad hoc data reporting services.

- **Ability to interface with other systems**--The use of the mainframe as the data base and applications host for this alternative limits the ability to interface with other systems. As the federal government and other state and local agencies move toward client/server systems platforms, use of the mainframe and its proprietary methods and protocols will make interfacing more complicated than it might be under other, more "open" circumstances.

- **Ability to incorporate future technologies**--The technology direction of the 1990's is founded on concepts such as "open" systems and client/server computing, with architectures based on non-proprietary computers and operating systems, and on inter-changeability of hardware and software from various vendors. The use of the mainframe, a proprietary, legacy-type systems environment, will limit the ability to incorporate emerging and future technologies.

- **Integration with the desktop environment**--The mainframe environment permits a basic level of integration with desktop PC environments. The tools available with ADABAS provide this integration. It is not likely, however, that developers will concentrate new development efforts on the shrinking mainframe market.

- **Ease of administrative operation**--The mainframe environment is over twenty years old, and is a very stable and mature platform. As in the security area, there are a large number of tools available for administering the mainframe environment. The centralized nature of mainframe processing will make administration easier.

- **Availability of skilled technical personnel**--The state government has used the mainframe for years. Many state and private-sector employees know the environment well.

- **Cost**--This alternative will cost a little less ($852,000, or 6% less than alternative #2), on a one-time basis than the next two. The 5-year totals for this alternative and alternative #3 has very little difference, and the recurring costs for alternative #3 are 48% lower than for this alternative. Both of the other alternatives have lower recurring costs, and can take advantage of "open" systems and client/server technologies.

- **Ease of migration from the current environment**--Because the current APSIN system resides on the state mainframe and is based on the ADABAS data base system, this alternative does not require migration to a different hardware platform.

- **Standards compliant**--The use of a mainframe computer as the host data base and applications environment makes it non-compliant with emerging "open" systems standards.

- **Level of technical risk**--Using the existing mainframe as the host for the data base and applications environment, as well as existing computer networks, makes this alternative a relatively low-risk undertaking.

- **Ease of use**--The mainframe terminal environment will restrict the developer's ability to take full advantage of tools available to produce user-friendly interfaces. Additionally, as new tools are produced, their focus will continue to gravitate toward the GUI-based, intelligent-desktop workstation. Tool kit developers probably will not concentrate new development on the shrinking mainframe market.

- **Ad hoc data access**--The ad hoc data access available with this alternative should suffice to provide enhanced services to the user community. The lack of a GUI environment, that would give users access to visual representations of their data, as well as provide for point and click queries, is a drawback. As stated above, developers probably will not concentrate new development efforts on the shrinking mainframe market.

- **Security**--The mainframe environment is over twenty years old, and is a very stable and mature platform. Many security products can be applied in this environment, making it the most secure.

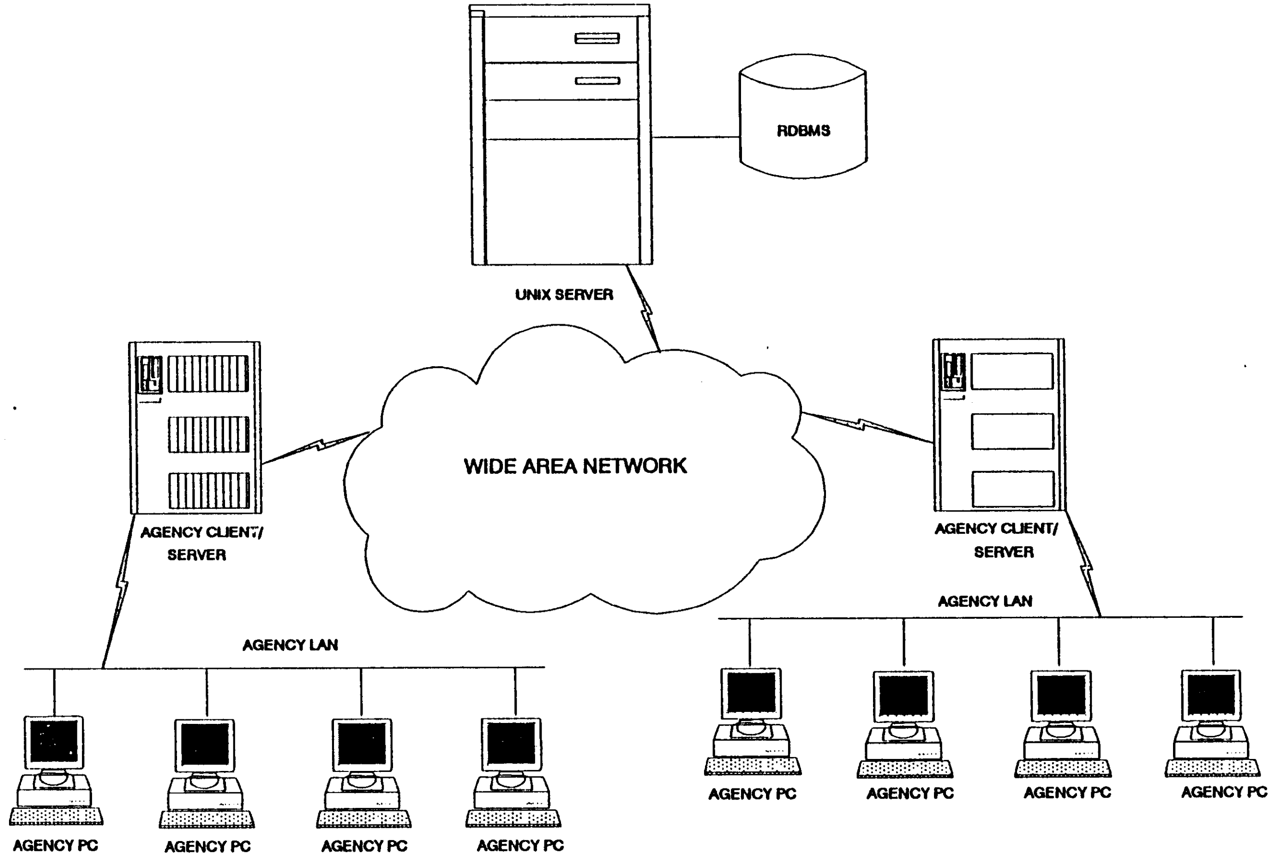
2. *Alternative 2--Full Client/Server Implementation Using a Unix-Based Server and an ANSI-Compliant Relational Data Base Management System, with Presentation via a Graphical User Interface*

This alternative is a full "client/server" implementation of the statewide systems using a relational data base management system and applications based on a graphical user interface, such as Windows or OS/2 Presentation Manager. Client/server is a computing architecture that has come to the forefront in the early 1990's. It represents a cooperative arrangement between workstation computers (clients) located on the desktop, that provide application program services; and larger computers (servers), that communicate with the clients via a network and provide data base, security, mail, and other services. Applications actually run on the client machines, and clients only connect to the servers when they require special services such as the processing of data base requests. A system schematic is presented as Figure 13 on the following page.

This alternative involves the rapid downsizing of existing mainframes and requires new applications that run on distributed client/server topologies. This alternative would be costly because it requires additional contract staff that would be required to perform the downsizing tasks quickly, and possibly quite chaotic for all agencies and users depending on the speed with which it was accomplished.

FIGURE 13

ALTERNATIVE 2
CLIENT/SERVER WITH
UNIX SERVER AND ANSI RDBMS



a. Technical Considerations

♦ **Computer hardware**--The computer hardware involved in a client/server architecture may vary widely. The client workstations in this environment are all computers, such as PC's, Mac's, or desktop Unix systems. No client can be a dumb terminal, as the application programs actually run on the client machines. The server machines generally provide only data base, security, and sometimes mail services. Such services may be implemented on many different types of machines. Thus, a server can be anything from a PC to a mainframe.

This alternative needs the following hardware:

- Client workstations--IBM-compatible PC's based on an Intel 80486 chip or better.

- Server system--Unix-based computer capable of providing data base services to several hundred concurrent users. Such a system might be based on a variety of currently available processing configurations, including RISC, symmetric multi-processing, or massively parallel processing.

♦ **Network**--The network that connects all the client computers to the server machine, as well as to each other, is the backbone of the client/server architecture. It must rapidly transfer data between the client and server machines to make the client/server model viable. The network associated with this alternative assumes that workstation PC's will connect to the statewide network via local networks (e.g., ethernet or token-ring), utilizing gateways to wide-area communications, and finally connecting to the server system. The statewide multi-protocol backbone would provide the wide-area links.

♦ **Operating system and utilities**--The client/server architecture should use a non-proprietary (open) operating system. Each possible operating system may be configured with a variety of utilities, including electronic mail and communications packages. For this alternative we assume the use of the Unix operating system. The Unix operating system has an open system orientation (although many computer hardware vendors use proprietary versions of Unix on their systems, which should be avoided) and easily permits applications and utilities to move across hardware from multiple vendors.

- **Data base**--The client/server model takes advantage of recent advances in data base technology. Specifically, RDBMS's (relational data base managers) can serve many users, letting them access data readily in a variety of ways.

- **Applications environment**--A GUI (graphics user interface, such as the Macintosh or Windows systems) makes full use of emerging technologies and expands the data and analysis available to users. A GUI makes it easier to move applications, and will let the state easily integrate statewide system data with PC-based applications such as spreadsheets and word processors.

  To develop applications in the GUI/RDBMS environment, we recommend using a fourth-generation language product that supports the selected GUI/RDBMS combination. Such a product will allow more efficient applications development and provide a standardized means of constructing user interfaces to the system. The fourth-generation language would be used together with a third-generation language, such as COBOL or C, to provide required programming capabilities that are not built into the fourth-generation product.

- **Cost components specific to this alternative**--Implementing a full client/server architecture in the current state data processing environment would be costly. It requires contracting for technical resources to assist in the rapid downsizing effort. It also would require a large Unix-based host computer, along with the associated relational data base management system, capable of supporting at least 250 concurrent system users. The cost of Oracle on an open system platform assuming 250 concurrent users is $327,000 versus $614,000 for Oracle on the mainframe. It also would need the statewide multi-protocol network, and deployment of powerful PC's for workstations.

For this alternative, the objective is to move all applications from the mainframes to client/server devices, and to pursue new applications that will operate in this technology environment. The departments of Law and Corrections would pursue package or custom-developed solutions, but only those that would operate in a client/server environment. The Alaska Court System would continue with its current strategy of system redesign and development; DPS would develop all new applications on a client/server, but transfer current applications to a server that has the ADABAS data base system so legacy applications can continue to operate without revision; and DOA/DIS would pursue the installation of a multi-protocol network.

Tables 6 through 10, on the following pages, detail our cost estimates for this alternative. Assuming this migration takes three years, full cost savings on DOA/DIS charges for mainframe time will not be seen until year four. The total one-time costs equal $16,407,000. Recurring costs over five years add up to a cost savings of $372,000. The total five-year cost is $16,035,000. Because of the speed of the downsizing effort, the recurring cost savings occur sooner than with alternative #3 but will be similar in size after year five.

DOA/DIS--For this alternative we suggest that the state acquire a large Unix host processor(s) housed at and managed by DIS. For the suggested client/server equipment, systems software and relational data base software we estimate one-time costs of $902,000. We have included two new staff resources to support this system and have included training costs for these two people. The one-time cost to implement a multi-protocol network over three years remains at $3,250,000.

TABLE 6

ALTERNATIVE 2
DEPARTMENT OF ADMINISTRATION, DIVISION OF INFORMATION SERVICES
($000)

PROJECT TASKS	FY 95		FY 96		FY 97		FY 98		FY 99	
	Recurring	One-Time	Recurring	One-Time	Recurring	One-Time	Recurring	One-Time	Recurring	One-Time
1. Acquire Hardware and Software and Install a Multi-protocol Network										
a. Statewide E-mail		300								
b. Network Management		160								
c. Statewide Internet		1,953		538.2		298.8				
2. Large Host Processor/Server and Network Components				475	48		50		52	
3. Relational Data Base Management System(s) and ADABAS				427	60		65		70	
4. New Staff Resources (2 FTE's)			<104>		<110>		<115>		<121>	
5. Staff Training				<40>		<40>				
TOTALS		2,413	<104>	1,400.2	<2>	258.8	-0-		1	

TABLE 7

ALTERNATIVE 2
DEPARTMENT OF PUBLIC SAFETY
($000)

PROJECT TASKS	FY 95		FY 96		FY 97		FY 98		FY 99	
	Recurring	One-Time	Recurring	One-Time	Recurring	One-Time	Recurring	One-Time	Recurring	One-Time
1. Migrate Current Systems to Host										
a. Migration Plan		75								
b. Transfer APSIN				2,750						
2. Criminal History Enhancement/Interfaces						600		500		
3. NCIC-2000										
a. Analysis and Design						225				
b. Implementation								500		
4. AFIS Replacement		500		500		500		500		
5. AFIS Live-Scan Devices (10)				487.5		487.5				
6. APSIN/AAFIS/NCIC Integration								250		
7. Network Enhancements		500		115		115				
8. DOA/DIS Rate-Based Service Charges										
a. Network										
b. Mainframe					<1,000>		<1,000>		<1,000>	
c. Host					250		270		290	
9. New Staff Resources (3 FTE's)			104		156		164		172	
10. Staff Training				100		100				
TOTALS		1,075	104	3,952.5	<594>	2,027.5	<566>	1,750	<538>	

TABLE 8

ALTERNATIVE 2
DEPARTMENT OF LAW
($000)

PROJECT TASKS	FY 95		FY 96		FY 97		FY 98		FY 99	
	Recurring	One-Time	Recurring	One-Time	Recurring	One-Time	Recurring	One-Time	Recurring	One-Time
1. System Re-engineering		75								
2. Alternatives Evaluation		15								
3. Rapid Prototyping				25						
4. System Acquisition/Implementation				200		100				
5. Equipment				50		50				
6. DOA/DIS Rate-Based Service Charges										
a. Network			15		20		20		20	
b. Host			30		40		40		40	
7. New Staff Resources (2 FTE's)			104		110		116		122	
8. Staff Training				40		40				
9. Elimination of Contract Programming Services			<25>		<25>		<25>		<25>	
TOTALS		90	124	315	145	190	151		157	

TABLE 9

**ALTERNATIVE 2
ALASKA COURT SYSTEM
($000)**

PROJECT TASKS	FY 95		FY 96		FY 97		FY 98		FY 99	
	Recurring	One-Time	Recurring	One-Time	Recurring	One-Time	Recurring	One-Time	Recurring	One-Time
1. Trial Court System Development Cost[1]		<200>		<225>						
2. Appellate Court System Development Cost						125		125		
TOTALS						125		125		

[1] This cost has already been appropriated.

TABLE 10

ALTERNATIVE 2
DEPARTMENT OF CORRECTIONS
($000)

PROJECT TASKS	FY 95		FY 96		FY 97		FY 98		FY 99	
	Recurring	One-Time	Recurring	One-Time	Recurring	One-Time	Recurring	One-Time	Recurring	One-Time
1. System Re-engineering		150								
2. Alternatives Evaluation		25								
3. Rapid Prototyping				50						
4. System Acquisition/Implementation				1,500		500				
5. Equipment				200		100				
6. Staff Training		40		60		60				
7. DOA/DIS Rate-Based Service Charges										
a. Network			30		50		55		70	
b. Host			90		140		150		165	
TOTALS		215	120	1,810	190	660	205		235	

DPS--For this alternative, we have retained the projects from the Information Systems Management Plan described in alternative 1, but have added a project to plan the migration from the mainframe to the Unix host processor(s), and to actually accomplish this transfer at a total cost of $825,000.

We have included the costs of a new AFIS system with thirteen live-scan devices at $2,975,000 over five years. Three of the live-scan devices are intended for use by DFYS for juvenile fingerprinting.

We have added the same number of new staff as described in alternative 1 but have increased the training expense to $200,000. We estimate that rate-based service charges from DIS will decrease substantially from the mainframe environment when recalculated based on the Unix host environment. We expect that network charges would continue at their current levels.

DOL--As with alternative 1, the DOL costs include creating a two-person data processing staff and replacing PROMIS with a new system. We estimate that a client/server-based system will cost less than a mainframe version. We expect that the DIS rate-based service charges for the Unix host processor will be substantially less than on the mainframe.

Alaska Court System--The court system scenario under this alternative stays the same as alternative 1.

DOC--As with DOL, under this alternative the DOC would procure a new system that would run on a client/server system. We estimate this will cost less than a mainframe version. We also estimate the rate-based service charges from DIS will be substantially less.

- **Significant issues**--Client/server computing is an emerging computer architecture, setting the direction of computing in the 1990's. Implementing a true client/server system calls for the interconnection, control, and coordination of all computers connected to the agency system, a difficult task at present. It will not work with dumb terminals. If the state selects this alternative, all users of the repository would need access through a network-connected PC workstation.

b. Evaluation Criteria Applied to Alternative 2

The following discussion details how this alternative complies with each of the technical-alternatives rating criteria.

- **Ability to meet basic system requirements**--This alternative uses an ANSI-standard relational data base, running in a true client/server environment. This alternative can completely meet the basic requirements of the CCH repository. Further, it will run on the widest range of computer hardware platforms, and gives the most flexible tools, e.g., query, browse, and reporting, to the system users.

- **Ease of use**--This alternative allows developers to design and implement a very user-oriented, easy-to-operate system. Many tools are available now, and vendors are introducing new ones for creating graphical user interfaces on client/server systems. GUI interfaces are easy to understand, and allow users to inter-operate with other components of their desktop environment.

- **Ad hoc data access**--A wide variety of ad hoc data query tools are available for RDBMS's. Operating in a desktop GUI environment will allow such tools to take advantage of visual representations of data structures, providing the easiest and most intuitive means of ad hoc data access.

- **Security**--Use of the client/server environment places processing power on the desktop of all system users. It also provides the highest degree of access to statewide data bases. While these features enhance user functionality, they also present many potential security problems. The data base system can provide security but because client/server is an emerging technology, add-on security tools are still not widely available.

- **Ability to interface with other systems**--The client/server architecture based on a relational data base system provides unlimited flexibility for interfacing with other systems. It meets emerging standards--both federal, and those outlined in this chapter--and allows connection to outside systems using a wide variety of methods.

- **Ability to incorporate future technologies**--Client/server architecture based on open systems and relational data base systems sets the emerging standard for new systems development. Because this architecture uses the latest computer technology, it can best take advantage of and incorporate future technologies as they are developed.

- **Integration with the desktop environment**--The client/server environment largely runs on the desktop. Through the use of a GUI and a variety of development tools, it operates similarly to the applications such as word processors and spreadsheets that are native to that environment. Such an architecture obviously will integrate well with the desktop environment.

- **Ease of administrative operation**--The client/server environment requires the administration of both data and applications code across many diverse computer platforms. It also introduces the complexity of operating via a wide-area network, and naturally reduces the controls available in a more traditional environment such as the mainframe. Although numerous vendors are working on solutions to these administration problems, adequate administration products and methods for this environment will take more time.

- **Availability of skilled technical personnel**--The client/server environment consists of very new technology. Relatively few technical personnel truly understand this architecture even though many businesses are introducing it. Additionally, the existing state data processing staffs have virtually no experience deploying such an architecture.

- **Cost**--A true client/server architecture conversion for the criminal justice system would be costly with regard to one-time contract technical services required. Also all desktop workstations would need to be powerful PC's with a variety of client software loaded. The state would have to acquire a statewide multi-protocol network and a powerful Unix host computer. State personnel would have to learn how to use this environment, which would increase costs. Relative to the other design alternatives, the one-time costs of a client/server conversion to a completely new environment would cost the most, as detailed earlier in this section.

- **Ease of migration from the current environment**--The client/server environment, based on an ANSI-standard RDBMS, is probably as different from the current APSIN processing environment as is possible. Migration from the current environment would be complicated by such an architecture.

- **Standards compliant**--Of all the alternatives presented, the client/server architecture based on an RDBMS conforms most closely to emerging computing standards. Deployment of such an architecture would ensure that the statewide systems match the stated technology direction of the federal government and state enterprises including the Alaska Court System.

- **Level of technical risk**--Companies are just beginning to use client/server architectures and depend on a wide variety of emerging hardware, software, and networking technologies. Very few technical personnel have real experience working with client/server technologies. The use of such an architecture has a high degree of inherent technical risk. This is particularly true for this alternative because of the rapid conversion to client/server which will be disruptive to normal operations and costly in the short-term to achieve full conversion.

3. *Alternative 3--Session Server/Data Base Server Using a Unix-Based Operating System and an ANSI-Compliant Relational Data Base Management System Combined with a Mainframe Data Base Server with ADABAS*

Alternative 3 applies 1990's technology to the CCH repository by providing a route toward client/server systems. It allows the possibility of future migration to full client/server computing, while simultaneously preserving the current investment in mainframe technology. This alternative relies on Unix terminal sessions running on one computer, an RDBMS on this server for new applications, and the continued use of existing legacy data base applications on the mainframe. A system schematic appears in Figure 14 on the following page. This incremental migration would be more successful than the monumental migration described in Alternative 2, because all the risks and tasks associated with it can be contained in small subsets of the entire migration effort.

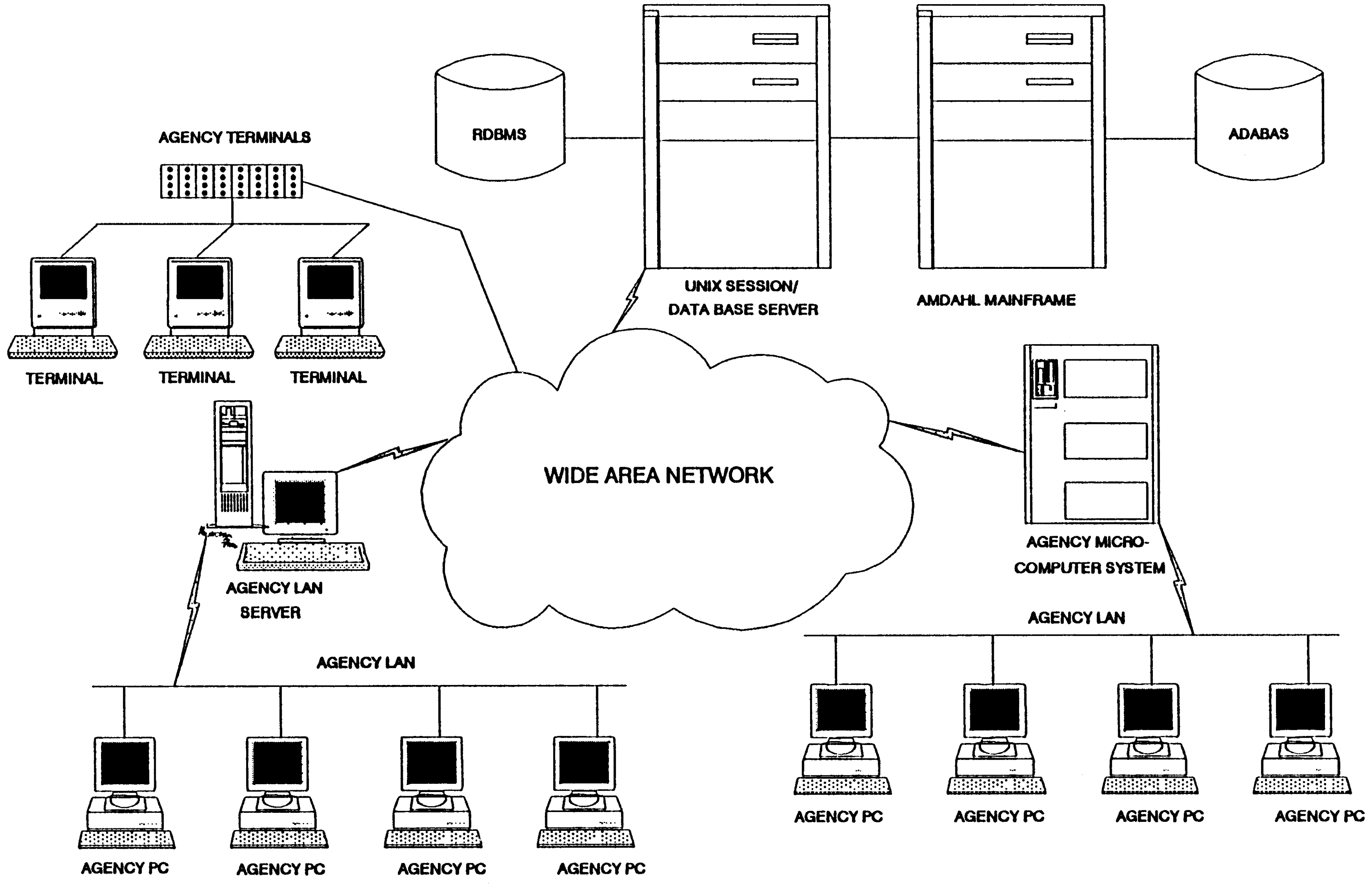
a. Technical Considerations

- ♦ **Computer hardware**--The computer hardware for this alternative consists of one large Unix-based computer as a server for new or transferred applications, and the continued use of the mainframe as a data base server for specific client applications. The Unix system might be based on a variety of currently available processing configurations, including RISC, symmetric multi-processing, and massively parallel processing.

- ♦ **Network**--The network required by this alternative should support the connection of existing PC's and dumb terminal workstations to the Unix server system or the mainframe, depending on the application and the data base location. Such a network would allow connection to the Unix system from PC's attached to local agency networks and 3270-type terminals attached to any of the mainframes.

FIGURE 14

ALTERNATIVE 3
UNIX SESSION/DATA BASE SERVER WITH RDBMS/ MAINFRAME DATA BASE SERVER WITH ADABAS



- **Operating system and utilities**--This alternative uses a Unix operating system for the server, with an associated utility package that allows interconnection of existing mail and other systems running on current agency platforms. The Unix operating system has an open system orientation (although many computer hardware vendors use proprietary versions of Unix on their systems, which should be avoided), and easily allows applications and utilities from multiple vendors to move across hardware. The MVS operating system and present utilities will continue to be used on the mainframe.

- **Data base**--This alternative uses an ANSI-standard relational data base management system on the Unix server and continues to use ADABAS on the mainframe. Users would reach these data bases through straight SQL (Structured Query Language).

- **Applications environment**--Because this system connects dumb terminals to the mainframe, it needs a "lowest-common-denominator" textual interface (ASCII). A fourth-generation language working together with a relational data base manager can develop applications more efficiently, and in a more standardized style. Replacing all dumb terminals with PCs should be a long-term goal.

  If the selected development tool automatically generates both character-based and graphical interfaces from the same application code, then intelligent workstations (PC's) connected to the network could have the advantages of a GUI, while a character-based, dumb-terminal interface would also be provided. The fourth-generation language would be used in conjunction with an appropriate third-generation language, such as COBOL, to provide required programming capabilities that are not built into the fourth-generation product.

- **Cost components specific to this alternative**--This alternative requires procuring and installing a new Unix-based host computer in the state's data processing environment. It also requires acquisition of the associated ANSI-standard relational data base system and upgrades to existing network systems. As with the previous alternative, all new applications (e.g., for departments of Law and Corrections), whether package or in-house developed, will be processed for the "open" system environment. Existing DPS applications will remain on the mainframe. DPS can move them gradually, as time and costs permit, and as practical considerations, such as response time, are accommodated.

Tables 11 through 15, on the following pages, detail our cost estimates for this alternative. Because the DPS applications will stay on the mainframe for the foreseeable future, the Unix host can be smaller and less costly than in Alternative 2. The DPS applications would not begin to migrate to the client/server host system until at least year five. The one-time costs for Alternative 3 come to $14,857,000, with recurring costs estimated at $2,023,000 over five years. The total is $16,880,000. The recurring costs will continue to decrease after year 5 because of reduced rate-based service charges once the conversion to client/server is completed.

DOA/DIS--For this alternative, the client/server host processor will be smaller and less costly than the system suggested for Alternative 2, approximately $702,000 versus $825,000, but DIS could still house and manage it. We have included two new staff to support this system, and their training costs. The one-time costs to implement a multi-protocol network over three years totals $3,250,000.

DPS--For this alternative, we still retain the projects from the Information Systems Management Plan described in the previous two alternatives, but have added, late in the plan, a project to plan the migration from the mainframe to the Unix host processor(s). DPS should rewrite the migrating applications to use the relational data base and tool set on the "open" system to maximize the connectivity and operability of all the criminal justice systems. This approach will require substantial funding.

TABLE 11

ALTERNATIVE 3
DEPARTMENT OF ADMINISTRATION, DIVISION OF INFORMATION SERVICES
($000)

PROJECT TASKS	FY 95		FY 96		FY 97		FY 98		FY 99	
	Recurring	One-Time	Recurring	One-Time	Recurring	One-Time	Recurring	One-Time	Recurring	One-Time
1. Acquire Hardware and Software and Install a Multi-protocol Network										
a. Statewide E-mail		300								
b. Network Management		160								
c. Statewide Internet		1,953		538.2		298.8				
2. Large Host Processor/Server and Network Components				375						
3. Relational Data Base Management System				327						
4. New Staff Resources (2 FTE's)			<104>		<110>		<115>		<121>	
5. Staff Training on Client/Server				<40>		<40>				
TOTALS		2,413	<104>	1,200.2	<110>	258.8	<115>		<121>	

TABLE 12

ALTERNATIVE 3
DEPARTMENT OF PUBLIC SAFETY
($000)

PROJECT TASKS	FY 95		FY 96		FY 97		FY 98		FY 99	
	Recurring	One-Time	Recurring	One-Time	Recurring	One-Time	Recurring	One-Time	Recurring	One-Time
1. Criminal History Enhancement/Interfaces				600		500				
2. NCIC-2000										
a. Analysis and Design		225								
b. Development/Implementation				500						
3. AFIS Replacement		500		500		500		500		
4. AFIS Live-Scan Devices (10)				487.5		487.5				
5. APSIN/AAFIS/NCIC Integration						250				
6. Network Enhancements		500		115		115				
7. DOA/DIS Rate-Based Service Charges										
a. Network										
b. Mainframe			200		300		300		<500>	
c. Host									250	
8. New Staff Resources (3 FTE's)			104		156		164		172	
9. Staff Training								50		50
10. Migrate Redeveloped Systems to Host										
a. Migration Plan								75		
b. Transfer										1,500
TOTALS		1,225	304	2,202.5	456	1,852.5	464	625	<78>	1,550

TABLE 13

ALTERNATIVE 3
DEPARTMENT OF LAW
($000)

PROJECT TASKS	FY 95		FY 96		FY 97		FY 98		FY 99	
	Recurring	One-Time	Recurring	One-Time	Recurring	One-Time	Recurring	One-Time	Recurring	One-Time
1. System Re-engineering		75								
2. Alternatives Evaluation		15								
3. Rapid Prototyping				25						
4. System Acquisition/Implementation				200		100				
5. Equipment (PC's and Network)				50		50				
6. DOA/DIS Rate-Based Service Charges										
a. Network			15		20		20		20	
b. Host			30		40		40		40	
7. New Staff Resources (2 FTE's)			104		110		116		122	
8. Staff Training				40		40				
9. Elimination of Contract Programming Services			<25>		<25>		<25>		<25>	
TOTALS		90	124	315	145	190	151		157	

TABLE 14

ALTERNATIVE 3
ALASKA COURT SYSTEM
($000)

PROJECT TASKS	FY 95		FY 96		FY 97		FY 98		FY 99	
	Recurring	One-Time	Recurring	One-Time	Recurring	One-Time	Recurring	One-Time	Recurring	One-Time
1. Trial Court System Development Cost[1]		<200>		<225>						
2. Appellate Court System Development Cost						125		125		
TOTALS						125		125		

[1] This cost has already been appropriated.

TABLE 15

ALTERNATIVE 3
DEPARTMENT OF CORRECTIONS
($000)

PROJECT TASKS	FY 95		FY 96		FY 97		FY 98		FY 99	
	Recurring	One-Time	Recurring	One-Time	Recurring	One-Time	Recurring	One-Time	Recurring	One-Time
1. System Re-engineering		150								
2. Alternatives Evaluation		25								
3. Rapid Prototyping				50						
4. System Acquisition/Implementation				1,500		500				
5. Equipment				200		100				
6. Staff Training		40		60		60				
7. DOA/DIS Rate-Based Service Charges										
a. Network			30		50		55		70	
b. Host			90		140		150		165	
TOTALS		215	120	1,810	190	660	205		235	

We have included the costs of a new AFIS system and thirteen live-scan devices at $2,975,000 over five years. Three of the live-scan devices are intended for use by DFYS for juvenile fingerprinting.

We have added the same numbers of new staff as described in the previous two alternatives and have included $100,000 in training expenses. Agencies would continue to incur the estimated rate-based service charges until such time as the applications are transferred to the Unix server, at which time the costs should decrease substantially.

DOL--As with Alternative 2, the DOL costs include creating a two-person data processing staff and replacing PROMIS with a new system. We estimate that a client/server-based system will cost less than a mainframe version. We also would expect the DIS rate-based service charges for the Unix host processing to be substantially less than on the mainframe.

Alaska Court System--The court system scenario stays the same as in alternatives 1 and 2.

DOC--As with DOL, under this alternative the DOC would procure a new system running on a client/server system. We estimate that this will cost substantially less than a mainframe version. We also estimate that the rate-based service charges from DIS will be substantially less.

♦ **Significant issues**--Introducing Unix server systems into the state data processing environment will be costly, because the state must buy new hardware and software and must train staff to develop applications in and support the new environment. A Unix server configuration will, however, position the state to take advantage of the emerging technologies of the 1990's. From a purely technical perspective, this alternative is probably the most attractive. It maximizes the use of existing equipment, while providing the benefits of a fully relational DBMS and presenting a clear migration path to open systems and client/server architectures in the future. The alternative, however, will require a very significant investment in computer and network hardware, in new software, and in retraining of systems development and support personnel.

b. Evaluation Criteria Applied to Alternative 3

The following discussion details how this alternative complies with each of the technical-alternatives rating criteria.

- **Ability to meet basic system requirements**--This alternative implies an ANSI-standard relational data base and a standards-compliant, Unix-based host computer system for all new applications. It allows a wide choice of computer platforms on which to run the system, and supports a large number of tool sets for developing the applications and providing ad hoc data services.

- **Ease of use**--The state would implement this alternative using a fourth-generation language applications development tool that works in conjunction with the selected RDBMS. These products will allow the development team to build new agency systems that incorporate many of the "Ease-of-Use" features required. Simple navigation through the applications, easy queries and reporting, and built-in ad hoc features all will be available.

- **Ad hoc data access**--The ANSI-compliant RDBMS allows use of the many ad hoc data access tools available for this environment.

- **Security**--The Unix environment does not have the wealth of system and session security products that exist for the mainframe processing environment. However, the RDBMS systems do provide a significant security scheme. By the time the new systems are developed, many new Unix security products probably will be available.

- **Ability to interface with other systems**--The Unix systems environment is the cornerstone of the computer industry's current movement to open systems. Unix systems interface with many computing platforms including the mainframe, and many products help provide open access. RDBMS systems integrate easily with other data base platforms. The court system, one of the main criminal justice agencies, is currently redeveloping its trial court applications, using Unix and PROGRESS RDBMS.

- **Ability to incorporate future technologies**--The Unix/RDBMS environment anchors a widespread move toward "open" systems. New technologies generally are conceived and built around this new computing paradigm. This alternative, therefore, takes maximum advantage of new technologies as they emerge.

- **Integration with the desktop environment**--The Unix/RDBMS environment proposed by this alternative will provide a reasonable level of integration with desktop PC environments. Largely, this integration comes with a wide variety of tools available with the RDBMS component of the solution.

- **Ease of administrative operation**--The Unix/RDBMS environment of this alternative requires administration of multiple levels of systems and applications software. Both the Unix and RDBMS products envisioned provide a variety of administrative tools. The Unix operating system itself will complicate system administration. In addition, the state will have to continue maintaining the mainframe.

- **Availability of skilled technical personnel**--Even though many businesses currently use Unix/RDBMS technology, Alaska does not have many skilled technical personnel to service this environment. More will become available in time because of the rapid growth of these technologies.

- **Cost**--This alternative uses new hardware and software, as well as the mainframe. This costs a little more than alternative 2 in the short-term(assuming that the rate-based savings projection is accurate), but a little less than alternative 1.

- **Ease of migration from the current environment**--The current mainframe-based CCH repository environment uses ADABAS/ NATURAL, which differs from the Unix/RDBMS solution proposed for this alternative. Migrating from the current environment to the Unix/RDBMS configuration would be quite complex and costly, particularly since we recommend that the state re-develop the mainframe applications rather than transfer them.

- **Standards compliant**--The Unix/RDBMS portion of the solution complies completely with the existing open systems standards and with those that currently are being defined.

- **Level of technical risk**--Even though the Unix operating system has existed for almost twenty years, using Unix with an RDBMS, and extensive networks, is still a relatively new technology. New technologies have some degree of risk.

E. Recommended Alternative

We recommend that the criminal justice agencies pursue Alternative 3. This alternative introduces new technologies for all new applications, while preserving the state's investment in the mainframe where current applications would continue to reside. The eventual full migration from the mainframes could occur as time and budgets permit and the new technologies demonstrate they can support all these legacy applications.

To implement this alternative, the state should take these steps, among others:

- The DOA/DIS should implement a multi-protocol network as quickly as funding permits.

- Agencies should develop and promulgate the new standards discussed in this plan. The standards should include policies such as no longer purchasing 3270-type devices, and replacing existing ones as soon as possible.

- All criminal justice information systems should reside on "open" systems hardware and software.[122]

- All new applications, whether purchased packages or developed in-house or with contract staff, should use the new technologies. This includes new case management systems for the departments of Law and Corrections, the Alaska Court System, and all new applications for the DPS.

- DPS should enhance the criminal history repository on the mainframe with the new data elements and features described in this plan.

- All other DPS applications will remain, in the short-term, on the mainframe, in order to ensure service delivery, security, and response time requirements. DPS and agencies will develop interfaces to all agency systems for inquiry and updating purposes. Within the implementation period described in Chapter VIII and when the above tasks have been achieved, the entire DPS application will be downsized to an "open" system environment using a RDBMS and related tool sets compatible with the other criminal justice agency systems.

[122] The logical integration of systems using an RDBMS is straightforward. For example, the next release of Oracle will enable full replication, meaning that an update to one system automatically updates the other systems. Network traffic can be reduced by dispersing data base files. The criminal history repository could automatically query operational systems and retrieve updates made after the time of the last query. While ADABAS will continue as the data base supporting the legacy DPS mainframe applications, straight SQL access will insure interoperability.

Specific tasks related to implementing this recommended alternative are described in Chapter VIII. In this chapter, we have detailed a five-year implementation period that will require $14,857,000 in new one-time costs and $2,023,000 in new recurring costs.

Chapter VIII

Implementation Plan

This chapter explains how the criminal justice agencies should integrate their criminal justice information systems and improve the criminal history repository. The chapter first discusses underlying assumptions, and then describes the detailed projects for each agency for the next five fiscal years.

This plan assumes the funding and staffing needed for the tasks presented in the Gantt charts in this chapter. If the state delays funding or staffing the projects, agencies should modify the schedule according to the suggestions contained in Section D.

A. Plan Assumptions

Creation of this schedule required that we assume that the legislature and justice agencies will make several structural changes. These include:

- The legislature will pass the pending bills related to criminal justice information.
- The agencies will agree which agency (or new organization) will provide the leadership and oversight explained in Chapter III.
- Agencies will develop standards for client/server system, distributed systems, and system interfaces.
- Agencies will continue to cooperate and agree about the plan tasks and schedule.
- The legislature and agencies will fund the tasks laid out in the plan.
- The legislature and agencies will establish, fund and fill the new positions described in the plan.

Any changes in these underlying assumptions will require adjusting the proposed schedules.

B. Implementation Plan

This section sets out the Gantt charts for each agency that depict major project activities over the next five years. The five major agencies detailed here include the Department of Administration, Division of Information Services (DOA/DIS); Department of Public Safety (DPS); Department of Law (DOL); Alaska Court System (ACS); and the Department of Corrections (DOC). A discussion of efforts the smaller agencies should undertake follows the section on the larger agencies.

1. Department of Administration, Division of Information Services

Chart 1, on the following page, shows the project tasks for DIS over the next five years.

a. FY 1994-1995

In the first year DIS needs to develop standards for client/server and distributed systems. Working with the TIC and key agency representatives, the DIS should set standards for all procurements of these systems to ensure system interoperability.

DIS should begin a three-year process of building the multi-protocol network (statewide internet) that is an important component of this plan. DIS should start to establish two new positions to support large client/server systems that DIS houses and manages.

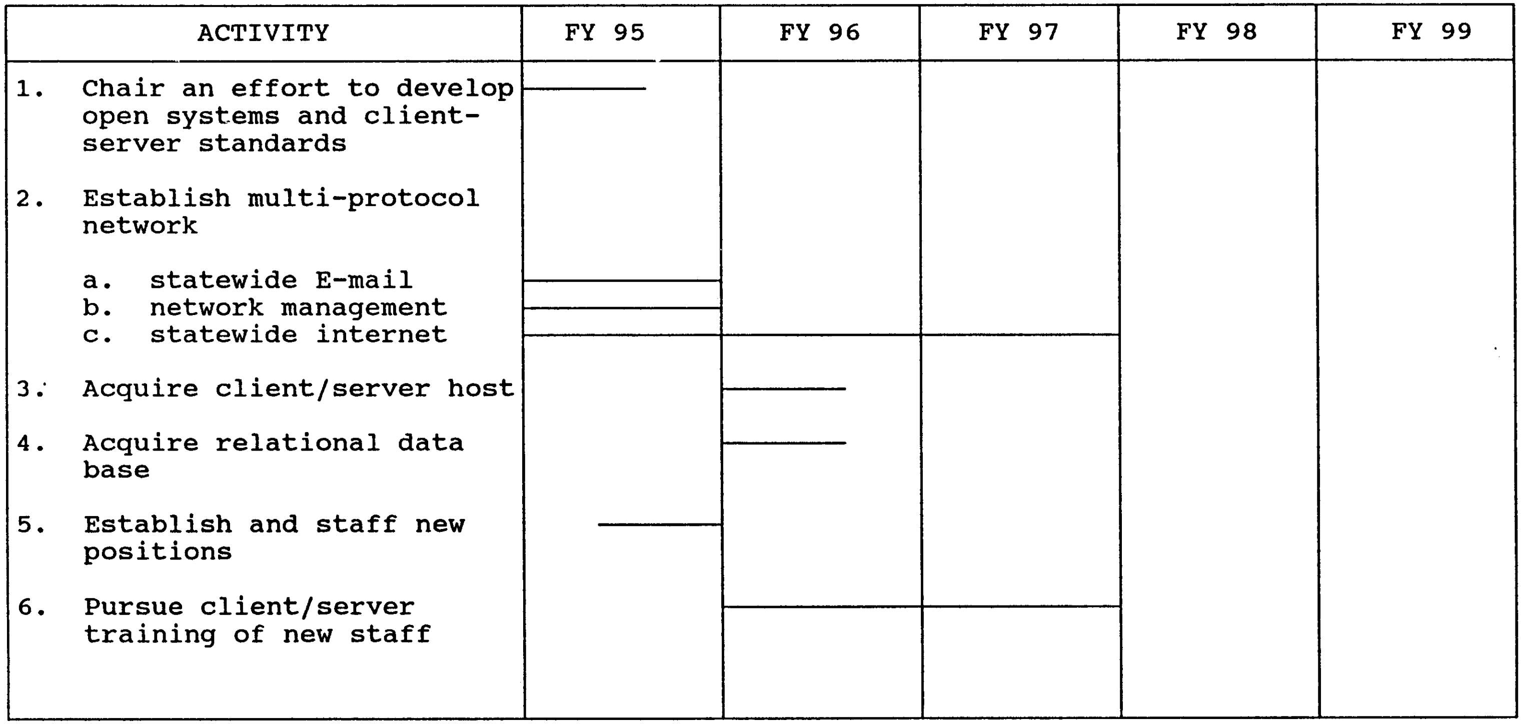
b. FY 1995-1996

DIS will continue to implement the statewide internet. Working with the criminal justice agencies, DIS will procure a client/server system large enough to accommodate new systems for the departments of Law and Corrections, and new applications for DPS. DIS should purchase a system that it can expand to accommodate all DPS systems if they eventually decide to convert to this architecture.

CHART 1

AGENCY IMPLEMENTATION SCHEDULE

DEPARTMENT OF ADMINISTRATION/DIVISION OF INFORMATION SERVICES



ACTIVITY	FY 95	FY 96	FY 97	FY 98	FY 99
1. Chair an effort to develop open systems and client-server standards	—				
2. Establish multi-protocol network					
a. statewide E-mail	—				
b. network management	—				
c. statewide internet	—	—	—		
3. Acquire client/server host		—			
4. Acquire relational data base		—			
5. Establish and staff new positions	—				
6. Pursue client/server training of new staff		—	—		

DIS should fill the two new positions and begin training all staff involved in supporting the client/server and distributed system technologies.

c. FY 1996-1997

This is the last year of the plan for DIS projects needed to integrate criminal justice systems and improve the criminal history repository. DIS will finish installing the statewide internet and will continue to train staff. Recurring costs include the new staff positions and maintenance on the client/server host.

2. Department of Public Safety

Chart 2, on the following page, shows project tasks for DPS over the next five fiscal years.

a. FY 1994-1995

The DPS has nearly a dozen projects during the five-year period, in addition to numerous other ongoing projects, and continued maintenance for existing systems. In the first year, DPS should analyze the impact of NCIC-2000[123] on the criminal history repository, and redesign the repository to meet NCIC needs. The department should begin to replace AAFIS and acquire more live-scan devices. (three of these live-scan devices are intended for DFYS to use to fingerprint juveniles.) The department should expand its network as envisioned in its Information Systems Management Plan. The department should work with the other criminal justice agencies, especially the courts, to incorporate the additional CCH data elements described in Chapter VI, and to develop a standard format for exchanging this information among criminal justice systems.

[123] NCIC-2000 (see Chapter II, *supra*) upgrades the NCIS to permit electronic transmission of identification information.

CHART 2

AGENCY IMPLEMENTATION SCHEDULE

DEPARTMENT OF PUBLIC SAFETY

ACTIVITY	FY 95	FY 96	FY 97	FY 98	FY 99
1. NCIC-2000					
a. analysis and design	—				
b. develop/implement		—			
2. AFIS replacement	—	—			
3. AFIS live-scan devices		—			
4. Criminal history enhancement/interface	—	—	—		
5. APSIN/AAFIS/NCIC integration			—		
6. Develop interface standards	—				
7. Network enhancements	—	—	—		
8. Establish and staff three new positions		—			
9. Conduct client/server training				—	
10. Migrate redeveloped systems				—	—

b. FY 1995-1996

During the second year DPS will finish replacing AAFIS and purchasing live-scan devices. DPS should examine developments in the AFIS industry that support an open systems approach and statewide live-scan implementation. Second, DPS should complete the NCIC-2000 enhancements to the criminal history repository, should build the enhancements detailed in this plan into the data base, and should begin to design interfaces with the new systems acquired by the departments of Law and Corrections.

Finally, the department should continue to enhance its network, and should establish and fill the three new staff positions necessary to support the new and ongoing project efforts.

c. FY 1996-1997

In the third year DPS will complete all enhancements of the criminal history repository, and of its network.

d. FY 1997-1998 and 1998-1999

During years four and five, DPS should consider moving its existing legacy systems to the client/server architecture. For at least the first three years of the plan, we believe the current DPS systems should stay on the mainframe. In year four of the plan, we suggest the department review the technical feasibility and desirability of moving from the mainframe to client/server or distributed technologies.

If the department decides to move, it should redevelop the systems, using a relational data base and associated tool sets that ensure compatibility with the other criminal justice agency systems.

The department may decide to keep all or part of these systems on the mainframe and to only develop new systems in the client/server environment. We have included a training budget in the plan, should DPS pursue these new technologies and need further staff training.

3. Department of Law

Chart 3, on the following page, details the project tasks for DOL. We believe that DOL should finish most of the work of procuring and implementing a new system during the first two fiscal years of the plan.

a. FY 1994-1995

In the first fiscal year, the department should begin to re-engineer the system. The design of a system to replace PROMIS should build on the business and functional models for a criminal case management system. The data and application architectures should, in turn, grow from that model. We believe that the department must complete this work in order to successfully design and procure a new case management system.

Next, DOL should choose between a packaged program and custom development of an application. Since the department will need data processing staff to support a new system, it should begin to establish two new positions.

b. FY 1995-1996

During the second year, the department should create or acquire a prototype of the new system to test; then buy or develop the application and install it on the new hardware procured by DIS. The department also should buy the PC and network hardware needed for the new system, fill the two new positions, and begin training staff in the new technologies.

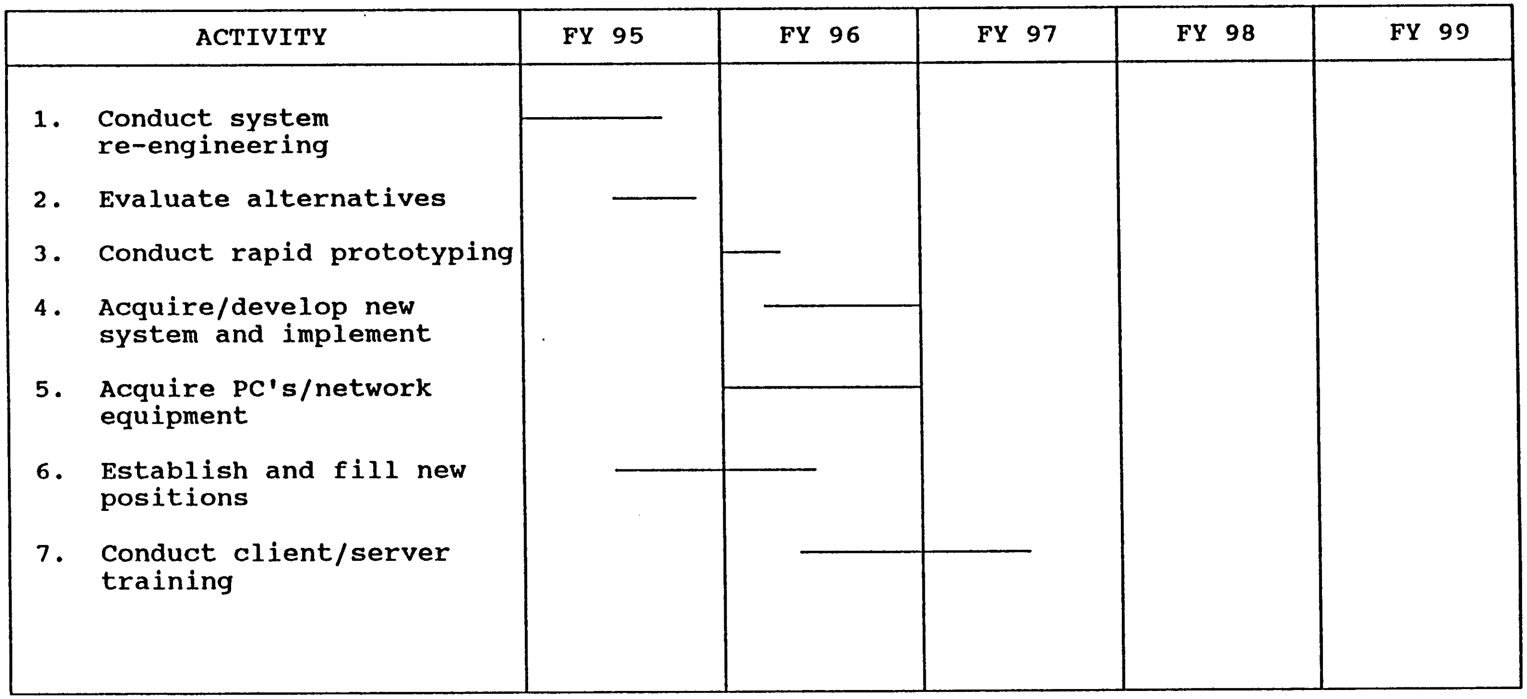
c. FY 1996-1997

For this third fiscal year, the DOL should complete any carryover tasks related to installing the system, procuring equipment, and training staff.

CHART 3

AGENCY IMPLEMENTATION SCHEDULE

DEPARTMENT OF LAW



4. Alaska Court System

Chart 4, on the following page, shows the project tasks for the court system. The court system has two major projects, each estimated to take two fiscal years to complete.

a. FY 1994-1995 and 1995-1996

In these first two fiscal years, the Alaska Court System will finish installing its new trial court system. Completing the criminal module will enable the court to electronically transmit offense disposition data to the criminal history repository. The criminal module should be complete by the end of FY 1996. While developing the system, the court should address the content, format, and method for electronically submitting and updating data in the criminal history record.

b. FY 1996-1997 and 1997-1998

The court has designed a new Appellate Case Management system. It expects to take two years to implement this system, and build an interface with the criminal history repository. While developing the system, the court should address the content, format, and method for electronically submitting and updating data in the criminal history record.

5. Department of Corrections

Chart 5, on the following page, details the project tasks for DOC. As with DOL, this department should replace its case management system (OBSCIS). Many of the tasks planned for the first three years relate to the replacement of this system.

a. FY 1994-1995

The department should begin the task of replacing OBSCIS by re-engineering the system. As we discussed for DOL, the design should first define the business and function models for a criminal case management system, and then derive the data and application architectures. The design should support the data that must be included in the criminal history record, as well as define the interface to the CCH. Following this process will ensure a successful system design and purchase.

CHART 4

AGENCY IMPLEMENTATION SCHEDULE

ALASKA COURT SYSTEM

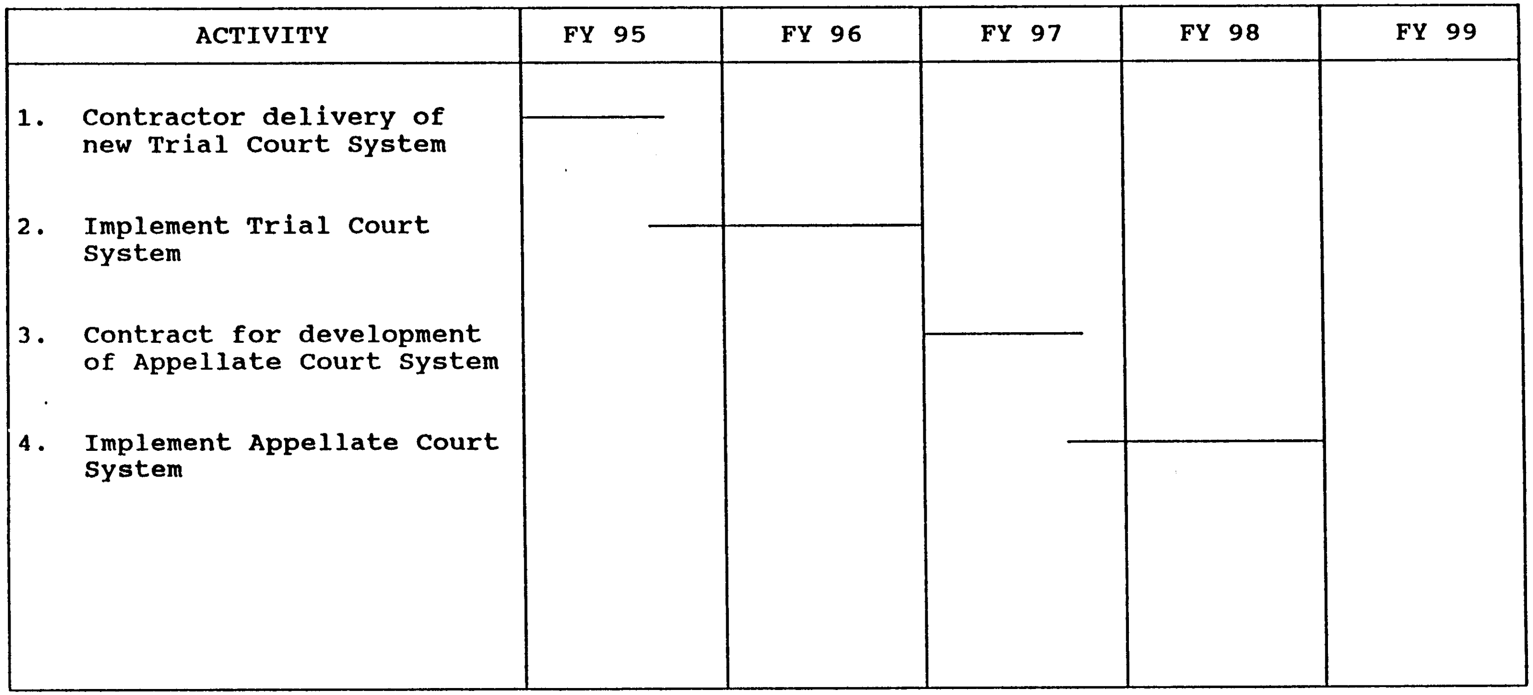
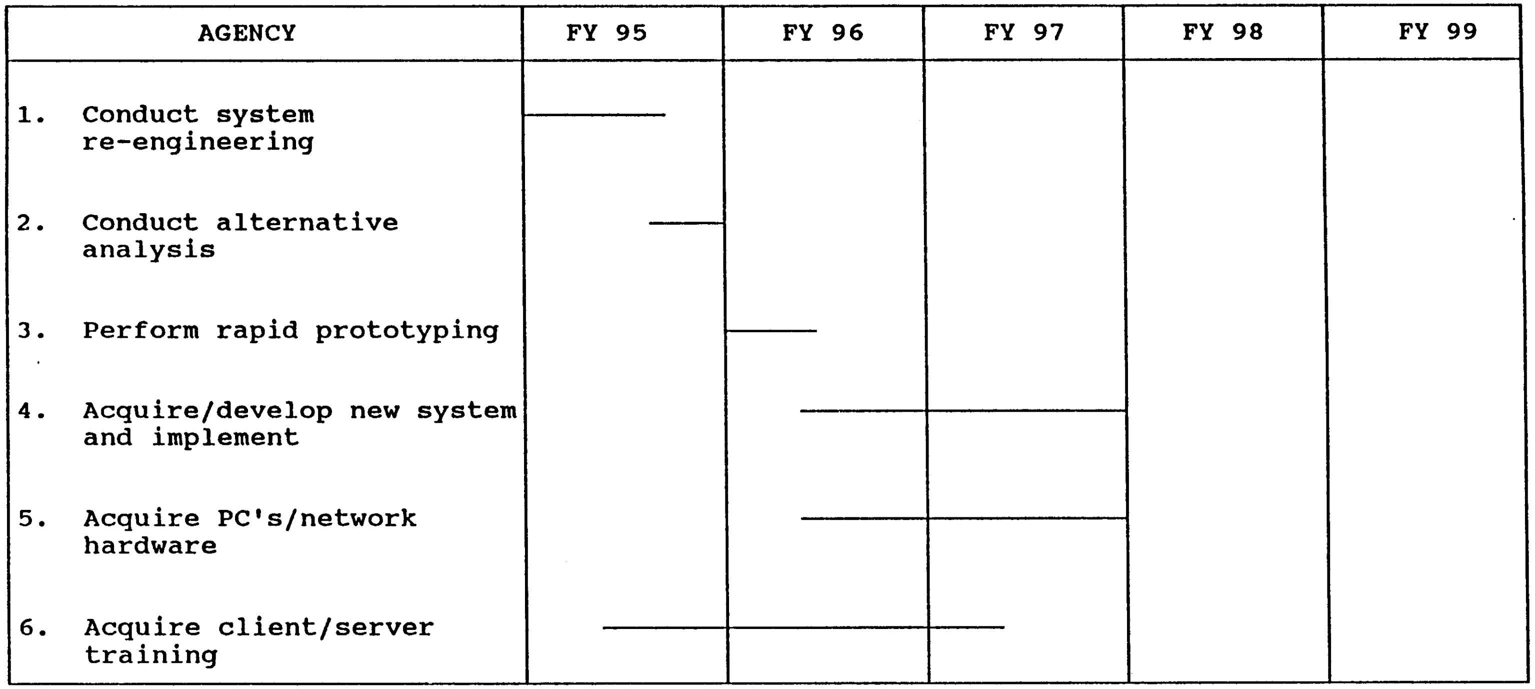


CHART 5

AGENCY IMPLEMENTATION SCHEDULE

DEPARTMENT OF CORRECTIONS



AGENCY	FY 95	FY 96	FY 97	FY 98	FY 99
1. Conduct system re-engineering	▬				
2. Conduct alternative analysis	▬				
3. Perform rapid prototyping		▬			
4. Acquire/develop new system and implement		▬	▬		
5. Acquire PC's/network hardware		▬	▬		
6. Acquire client/server training	▬	▬	▬		

DOC must assess the alternatives and decide between packaged and custom-built systems. The department must begin immediately to retrain data processing staff in the client/server and distributed system technologies that should underlie the replacement system.

b. FY 1995-1996

In the second fiscal year, the Department of Corrections should buy the new system by first prototyping the application, then buying or developing the system, and last, implementing the new software on the hardware procured by DIS. The department also should begin acquiring PC and network hardware needed to support the new system, and continue training staff in the new technologies.

c. FY 1996-1997

DOC should finish installing the new system and its interface to the criminal history repository. The department also should complete the purchase of hardware for the system and any remaining staff training.

C. Smaller Agencies

This plan has focused on the five major agencies in the criminal justice system. We documented the needs of several smaller agencies during the interviews and discuss them here. The agencies should complete thee tasks as time and funding permit.

1. Department of Health and Social Services, Division of Family & Youth Services (DFYS)

The DFYS is in the process of either analyzing the feasibility of or actually moving specific applications from the mainframe to a common PC platform. Staff are rewriting the PROBER primary client information system as a client/server application. The division is requesting additional state and federal funding to redevelop its entire set of systems using the new technologies.

These efforts should continue as funding permits. As DFYS begins to use these new applications, it should explore electronic interfaces to APSIN, Child Support, and OBSCIS.

The DPS budget includes funding for three live-scan devices to fingerprint arrested and adjudicated juveniles. DFYS should install these devices as soon as funding is available so that the department can record juvenile prints and transmit them to the AAFIS system.

2. Anchorage Police Department

The APD has developed a request for proposal (RFP) for a new police information system. Once APD has a new system, the selected vendor will need to help design an electronic interface to DPS that will give APD network access to the APSIN CCH repository, the Driver's License System, NCIC, and NLETS.

3. Anchorage Municipal Prosecutor

The Prosecutor's office needs to improve its criminal and driver history retrieval capabilities by developing network connections to APSIN. This prosecutor can create an interface by working with APD as it develops the electronic access to DPS discussed above.

4. Public Defender Agency

The PDA recently tied into APSIN and OBSCIS electronically through its network. This gives the agency sufficient access to these systems. The PDA should continue its efforts to implement its new case management system by the summer of 1994 in all its offices.

5. Alaska Judicial Council

As part of the Council's work in support of the Alaska Sentencing Commission, the Council developed a policy analysis data base through a complex process of criminal justice data extraction and matching using the existing criminal justice information systems.

The Council should continue to collect these data and enhance the data base by improving interfaces to the criminal justice systems as agencies acquire new applications. The Council's analyst should participate in any design activities for new systems, to insure that standards and designs consider the needs of the research data base that the legislature and other agencies call on to support policy decisions.

D. Alternative Implementation Activities if Funding is Delayed

As we explained in the Plan Assumption section of this chapter, these scheduled tasks cannot be accomplished without the funding described in Chapter VII. While the funding levels requested for FY 1994-1995 are limited, the lack of any funds would certainly delay the overall schedule. If the FY94-95 funds are not available, however, agency personnel could still move forward by continuing with ongoing projects and planning in anticipation of FY96 funds. These possible short-term activities are discussed below.

1. Department of Administration, Division of Information Services

Because the legislature may not fully fund the multi-protocol network at this time, the DOA/DIS, working with the Department of Labor is trying to implement an expanded multi-protocol network during the next fiscal year. Specifically, DOA plans to extend wide-area and SNA networks that will accommodate 56KB transmission rates to eleven additional cities, besides Anchorage, Fairbanks, and Juneau. These efforts should continue as funding permits.

The DOA/DIS also should chair a committee of criminal justice users to develop open system definitions for Alaska integrated justice information systems. The committee should complete its work by December 1994.

2. Department of Public Safety

The DPS should continue to develop a CRIMES system using client/server technologies. The legislature already has appropriated funds to develop and implement this system.

DPS should work with the other criminal justice agencies to agree on new CCH data elements, which agency will initially enter each element, and standards to the electronically exchange these data between systems.

3. Department of Law

The DOL must re-engineer its criminal case management before it can evaluate any new case management systems. This plan assumes that DOL would use consultant services to help with the re-engineering. If funding for a consultant is not available, DOL should seek assistance from the DPS data processing staff to conduct the re-engineering and design tasks.

4. Alaska Court System

The court system has made substantial progress in development of a new Trial Court case management system, using funds already allocated for this. The court schedule calls for the vendor to deliver the system modules over the next year. Although this schedule already is suffering some delays, efforts can continue for both development and implementation of this new system, regardless of plan funding.

While developing its new system, the court should work with DPS to define and develop standards for the electronic transfer of criminal history information to and from the repository.

5. Department of Corrections

Like DOL, DOC needs to re-engineer its case management system. This plan assumes that DOC will acquire consultant assistance with funding appropriated for the effort. If the legislature does not fund the project, DOC will need to delay this re-engineering effort until funding becomes available.

In the interim, the department should assign a member of its management team to oversee all automation projects, as well as to convey to department personnel a commitment to improved automation. Also, we recommend that the existing data processing staff not undertake any of the new project tasks since this staff does not currently have the technical or managerial expertise necessary to oversee or perform new systems design or development efforts that use new client/server technologies. Specific experience and expertise in these technologies is essential for these projects to be successful.

E. Conclusion

When the State of Alaska implements this plan, it will achieve what no other state has accomplished. Alaska will have a complete, accurate and timely criminal history repository integrated with the criminal justice agency information systems. Alaska will become a model for criminal history systems nationwide, with new ability to serve and protect the public through the effective use of technology.

Appendix A

Review of Literature

This appendix reviews national and Alaska literature on computer information system integration. The review is presented by agency and covers memoranda, minutes, and reports developed by the selected committees responsible for addressing integration issues.

A. National Literature

1. Electronic Fingerprint Transmission Specifications, Federal Bureau of Investigation, April 22, 1993

To support the FBI's Integrated Automated Fingerprint Identification System (IAFIS), the FBI in conjunction with the National Institute of Standards and Technology (NIST), has been developing a standard for electronically encoding and transmitting fingerprint image, identification, and arrest data. The standard (ANSI/NBS-ICST 1-1986) will define the content, format, and unit of measurement for the exchange of information that may be used in the fingerprint identification of a person. This standard will affect integrated systems planning in Alaska, because it will provide the common interface among state and federal fingerprint systems in the interchange between criminal justice agencies nationwide.

2. Integrated Automated Fingerprint Identification System (IAFIS) Planning Guide, Advisory Board to the National Crime Information Center of the Federal Bureau of Investigation, April 30, 1993

This planning guide describes IAFIS as a "paperless" computerized criminal history and fingerprint identification system under development by the FBI's Criminal Justice Information Services Division (FBI-CJIS). The three components of IAFIS are: the Interstate Identification Index (III), Identification Tasking and Networking (ITN), and the Automated Fingerprint Identification System (AFIS). When fully implemented, IAFIS will offer the capability of eliminating paper fingerprint cards at every step of the identification process. The ITM will handle workstations, workflow control, telecommunications, and fingerprint image files to support paperless identification processing.

See Chapter II, for a more detailed analysis of IAFIS as it relates to the integration effort of the State of Alaska.

B. Alaska General Literature

1. *Alaska Judicial Council*

a. *Governor's Criminal Justice Working Group Minutes*

The collected minutes of the Governor's Criminal Justice Working Group Minutes summarize the group's thinking about policy issues related to integrating Alaska's criminal justice information systems. The group coordinates justice system planning and makes recommendations to the legislature.

b. *Criminal Justice Computer Coordination Policy Group Minutes*

The Criminal Justice Working Group established this policy group to discuss policy issues relating to system integration and the Judicial Council's system coordination project. The collected minutes reflect problems and progress on these topics.

c. *Criminal Justice Information Systems Technical Users Group Minutes*

This group was created to advise the Computer Policy Group about technical computer information issues. The group has focused intensively on the data elements that each criminal justice agency wants to have included in the criminal history record, and the format standards for data elements in an integrated justice environment.

d. *State of Alaska Criminal Justice Statistical Data Base: December 1992. Justice Unified Statistical Data Base Operations Manual*

These documents reflect the efforts of the Alaska Sentencing Commission and the Judicial Council to take selected data from the separate criminal justice computer systems in order to create a statistical data base useful to the legislature, the executive branch and the judiciary in making policy decisions on criminal justice issues.

2. *Alaska Sentencing Commission*

a. *1992 Annual Report to the Governor and the Alaska Legislature, Alaska Sentencing Commission, December 1992*

The report focuses in large measure on the use of alternative punishments. It underscores the importance of the criminal history record as a source of information about the offender needed to decide on alternative punishments. See Chapter V, *supra* for further discussion of the importance of the criminal history record.

It also represents an important document for planning an integrated criminal justice system. To carry out the recommendations of the Sentencing Commission, the state's criminal justice systems will need to supply accurate, complete, and timely data to all agencies. The development of a comprehensive criminal justice data base is a key recommendation of the report.

3. *Department of Administration*

a. *Statewide Information Management Plan, March 1993 (Department of Administration/Division of Information Services)*

The Governor's Telecommunications Information Council requested this plan to design policies for managing the state's information resources and to guide State agencies. The Plan provides strategies for automated technologies, specifically data processing and telecommunications. Each agency controls and manages its own information resources.

b. *Data Network Review Study for ASPS No. 93-0145 (Alascom, Inc., 1993, Proposal)*

In its proposal, Alascom offered to perform work supporting the Alaska Data Network Project. Work would include assessing the current state network architecture, its operations, and associated costs; identifying short- and long-term network requirements; and recommending alternatives for network configurations and management.

c. Telecommunications Information Council 1993 Annual Report

In 1993, the TIC adopted three important objectives that will support the development of integrated justice information systems in Alaska: (1) develop a statewide telecommunications/information management plan; (2) establish institutional arrangements to implement improved information management in Alaska; and (3) establish information policies and guidelines to implement the plan. The TIC's goal is to comprehensively manage the state's information resources.

d. Visions of Alaska's Future—Development of a Statewide Telecommunications Network, Conference Report Goals and Recommendations. (Informatrix, Inc., March 1993)

The primary goal established at the conference was to initiate a planning effort for the development of a coordinated statewide telecommunications network. The goal was to have the network operating within three years. The key to the success of the planning process would be a comprehensive assessment of the needs and potential demand for telecommunications services in Alaska. The planning process also identified interoperability standards. These standards will play a major role in an integrated justice system. The conference reached consensus on goals, core principles, and recommendations for the TIC on establishment of a statewide network.

4. Department of Public Safety

a. "An Act relating to criminal justice information; and providing for an effective date,"—Proposed legislation to be enacted by the 18th Legislature of the State of Alaska and to be known as AS 12.62 [Introduced as HB442 and SB276]

The Act authorizes a criminal history record based on full arrest and disposition reporting by contributing agencies, and mandates fingerprint at critical stages of the justice process. See Appendix C, Commentary on APSIN Fingerprint Legislation, in this report for extended commentary on specific provisions of the Act as it relates to supporting integrated criminal justice information systems in Alaska.

b. *Alaska's Criminal History Records Supported by Fingerprints: Annual Survey of Completeness, December 1993. Records and Identification Division, Division of Administrative Services, Department of Public Safety.*

Based on criminal charges entered into APSIN in 1992, the survey found that "Alaska is doing a poor job of fingerprinting accused criminals." State Correctional facilities fingerprint less than 40% of offenders, while contract jails fingerprint about 50% of offenders. Smaller booking locations fingerprint only about 30 percent of offenders.

The report identifies three important initiatives that will improve fingerprinting: adopting AS 12.62 which mandates fingerprinting all offenders; funding Live-Scan Booking Terminals and replacing the current Automated Fingerprint Identification System (AFIS); and renewing the commitment of all parties who have responsibility for fingerprinting.

c. *Fingerprint Working Group, Meeting Notes, March 8, 1994*

The working group, representing the Departments of Corrections, Law, Public Safety, and the Anchorage Police Department, plans to identify problems in the state's criminal fingerprinting procedures. The group has identified the nature and extent of the problems, made specific assignments to investigate specific issues, and determined to meet regularly to resolve the fingerprinting problems.

d. *Alaska Criminal History Record Information Program: A White Paper. Lawrence C. Trostle, Justice Center, University of Alaska Anchorage, September 26, 1991. (JC #9203)*

The white paper covers the recommendations of SEARCH Group, general problems with the current criminal history system, and recommendations for improvement. The report focuses on the Eighteen Elements proposed by SEARCH to expand the range of events captured by the criminal history record. The paper calls for a distributed data tracking system and a legislative mandate to ensure capture of all key data elements. It concludes by recommending statutory authority for DPS to regulate the reporting of criminal arrest and disposition information.

e. *State of Alaska, Department of Public Safety, Information Systems Master Plan, ECG Management Consultants, August 1993*

This document provides a brief overview of a three-year tactical plan to improve information technologies within the Department of Public Safety. Its detailed tactical plan describes the current computing environment, the long-term (eight to ten years) strategic direction for DPS, and a series of short-term projects. It identifies the activities and resources required to design an open system environment in the DPS.

f. *Findings and Recommendations Concerning System Configuration. SEARCH Group, Inc., December 1, 1989*

This report presents findings measuring the performance of the Department of Public Safety information systems and procedures, and recommends changes. Areas covered include the data quality of records, completeness and timeliness of disposition reporting, and name search methods.

g. *Alaska Criminal History Record Processing—Baseline Assessment. SEARCH Group, Inc., March 31, 1993*

This document provides a baseline assessment of criminal history records maintained by DPS and makes specific recommendations for change. The assessment focuses on Alaska's compliance with the FBI Voluntary Reporting Standards for Improving Criminal History Information.

h. *Criminal History Record Repository Overview—Eighteen Points. SEARCH Group, Inc., March 23, 1992*

The overview proposes eighteen events that should contribute to and expand the criminal history record. See Chapter VI, Criminal History Record Data Elements, of this Strategic Plan for a discussion of the eighteen elements, and Alaska's state and federal reporting needs.

5. Department of Law

a. Criminal Justice Data base/Computer Coordination (Letter, June 13, 1993, from Dean J. Guaneli, Assistant Attorney General and Criminal Division Administrator, to William T. Cotton, Executive Director, Alaska Judicial Council)

DOL's PROMIS system runs on the state mainframe and costs about $50,000 per year in charge-backs to the Department of Administration. A maintenance contract for PROMIS software costs another $25,000 per year. At the time of this letter, DOL planned to improve its computer capability by transferring PROMIS data to another mainframe data base using BASIC-Plus, that would allow generation of statistical information. PROMIS data undergoes periodic purges because it exceeds its internal limit of one million records.

In the document, DOL supports the idea of a multi-agency integrated criminal justice system, linking agencies one by one, starting with the most compatible systems. DOL believed that further integrating the DPS and DOL systems would benefit them, and stated their preference for a joint system. Constraints to system-wide integration discussed include legal issues related to linking the courts, public defender, and prosecutor.

6. Department of Corrections

a. Systems Information for Criminal Justice Data base/Computer Coordination Project, 1993

This document describes current DOC hardware and software architecture. The department's current technology is the primary barrier to integrating DOC with other criminal justice agency systems. OBSCIS uses 1960s data processing methodologies and design. The system can only access data elements in a batch mode using a VSAM file design. Other barriers to integration included the few standard data elements or data entry formats, and lack of design/data base experience in the department. OBSCIS and HOFA cost $293,000 per year to maintain.

DOC plans in the future to upgrade aging telecommunications equipment, install tracking and accounting systems for critical statewide operations, assess its information needs, and develop an information system plan.

b. Alaska Department of Corrections Master Plan, Two Volumes, 1992 (Christopher Murray & Associates)

The comprehensive master plan focuses on operational and facility requirements during the 1990's. The plan examines factors that will affect offender population levels, and the recent geographical distribution of admissions and felony convictions.

The plan includes population projection that will affect planning for an integrated system. A no-growth forecast was projected in the 1990s, with Alaska's prison and jail population expected to be approximately 3,210 men and women in FY 1997. This is based on a 2.5 percent annual growth rate and peaking factor of six percent. The longer-range projected inmate population for the year 2010 is expected to be 4,264.

c. Review of Alaska Department of Corrections Master Plan Forecast, Second Draft (Allen Beck & Associates, February 26, 1993)

This report looks at how to improve the ability of the Department of Corrections to forecast its needs for bed space and resources. The report finds that the current DOC system, OBSCIS, has too little information to forecast jail and prison population growth. The report is important to the planning of an integrated criminal justice system in Alaska because it points out critical deficiencies in the current DOC automated system.

The number one recommendation of the report, in fact, calls for immediately improving the DOC automated system. The report elaborates, saying that the current system gives limited support to forecasting and other program planning and evaluation.

Other findings and recommendations aim to improve DOC's information systems. For example, to better control its population and to create more accurate forecasts, DOC should track offender subgroups. The integrated system should include the offender's status (e.g., parole, supervision, release, etc.) as part of the criminal history record and update.

The report also found that DOC does not have access to critical information about an offender from the systems of other justice agencies. As a result, DOC has not used crime data appropriately to create assumptions about population growth. This finding should be considered in establishing an interface to the CCH, and in defining the data elements to be included in the criminal history record. In general, the report highlights the inadequacy of the OBSCIS system.

d. Fiscal Impacts of SEARCH Bill (Memorandum, January 24, 1994, from Annette G.E. Smith, DP Manager, DOC, to Shirley Minnich, Director, Administrative Services, DOC)

This memorandum discusses the impact of the "APSIN Legislation" on the Department of Corrections. It focuses specifically on the amount of data that DOC might be required to provide to DPS should the commissioner of Public Safety be authorized to set responsibilities for data collection and delivery to DPS for the criminal history record. The memo objects to the requirement in the proposed legislation that DOC be responsible for obtaining a legible set of fingerprints. DOC viewed this requirement as a hardship on staff time.

The memorandum points to the inability of the current OBSCIS system to support an expanded criminal history record in an integrated systems environment. The memo also objects to reporting "at the time, in the manner, and in the form" that the DPS commissioner requires for reporting, as well as to "adopt reasonable procedures to ensure that criminal justice information that the agency maintains is accurate and complete." In short, the memorandum argues that virtually none of the requirements of the legislation could be met by the current automated system and operating procedures of DOC.

The report concludes with detailed staffing and data processing requirements; namely, the development of a comprehensive computer system for corrections, probation and parole. The cost is estimated at five million dollars.

e. *Report of Findings and Recommendations on the OBSCIS and HOFA Systems (Peat Marwick, author. Submitted by Mike Dindinger to Curt Wolfe, February 16, 1994)*

The essential finding of the report states that "The prisoner management and accounting systems are not widely used or relied upon by the staff of the Department [of Corrections]. The OBSCIS system does not provide the needed information capabilities for many uses. Few of the staff are properly trained in its use. The lack of consistent and accurate use of the prisoner tracking records system has lead to much duplicative work to maintain separate records either manually or on a personal computer." Citing the Cook Inlet facility as an example, the report says that eliminating these duplicative systems would save over 1.3 FTE or $45,000 per year in salary.

The report recommends that OBSCIS and HOFA undergo a major redesign to meet the operating needs of the Department; and says that once "a coherent central information management system is in place, all duplicative records must be eliminated." The report contains other recommendations, and an implementation approach for both short- and long-term improvements in the systems.

7. Alaska Court System

a. *Response to Criminal Justice Computer System Survey (Letter with attached document, December 17, 1993, from Richard W. Delaplain, Manager, Technical Operations, to William T. Cotton, Executive Director, Alaska Judicial Council)*

This document describes the court's current system including hardware, software, programming languages, and data base managers.

The court believed that the most significant barrier to systems integration was real-time access to multi-agency data bases, for purposes other than look-ups. The report also stated that the Court would have to reformat its data to transfer it to other agencies. Stored data formats may not match agreed-upon formats for transfer. The Court did not see this as a barrier to disposition reporting. A greater barrier noted was the set of strict prohibitions on access to court data, specifically juvenile information, psychiatric evaluations, and victim information. In general, the Court now obtains and shares information primarily in paper form.

Current and future technology plans include a total redesign of the trial court system. A three-year effort produced a general design document for the Court Information Processing System (CIPS). Moreover, an appellate court design has been completed. The CIPS system development project has been awarded and all modules are expected to be delivered by March, 1995. The report includes a detailed description of the AMA/ACS Development Schedule.

b. *General Design Specifications: Court Information Processing System (CIPS)—January 18, 1994*

The report gives detailed requirements for the CIPS criminal module, including key data elements in the information architecture. This design document shows that the system will include many elements needed in an integrated criminal history record, including charge tracking and full disposition reporting, appellate dispositions, and full sentencing information.

8. Anchorage Police Department

a. *APD Records Management System (PRMS) Request for Proposals (RFP) 1993*

The RFP asks for contractual services to set up a police records management system designed to interface with the existing PLIMS CAD and State APSIN system. The RFP includes, as secondary priorities, acquiring a Property & Evidence Tracking system, and a Computer-Aided Dispatching System. A full system replacement or extensive upgrade of current technology will be evaluated in the proposals.

9. Alaska Public Defender Agency

a. *Preliminary Plans for Computer Project (Memorandum, October 1, 1992, from Galen Paine and Blair McCune, Assistant Public Defenders, to Brian Duncan, Department of Administration)*

Reports on preliminary plans to improve computer and network capabilities in the Public Defender's Office, and to develop a case management system.

b. Description of Alaska Public Defender Agency Computer and Data base Systems (Memorandum, June 15, 1993, from Blair McCune, Assistant Public Defender, to William T. Cotton, Executive Director, Alaska Judicial Council)

This document reviews technology in the Alaska Public Defender Agency, and readiness for integration with other systems. Until the legislature provided funding for computer acquisition, the Agency had been limited to a small number of PC's acquired from the state surplus office, or brought in by attorneys who purchased their own computers and used them at work.

With $239,000 funding from the legislature, the Agency began installing a system of 386sx PC's on a 486 file server in Anchorage, with Fairbanks using Macintosh computers. One terminal in Anchorage connects to the state mainframe, mostly for accounting and administration rather than case management.

The Agency plans a case management system based on Microsoft FoxPro data base software. The Anchorage office will use a Novell network; Kenai will operate on a Lantastic network. Smaller offices will not use networks. The Agency also plans to install an e-mail network.

Barriers to integration include the Macintosh installation in Fairbanks and the low level of computer knowledge of staff members, especially in smaller offices. The agency expressed a need for direct access to current and past court cases, information, as well as complete, accurate, and timely information from the criminal history system.

c. Computerization Project (Memorandum, December 15, 1993, from Blair McCune, Assistant Public Defender, to John Salemi, Director, Public Defender Agency, Bob Stokes, Administrator, and all supervising attorneys)

Provides a progress report on automation efforts. WordPerfect was installed as the standard for word processing. Networking has been implemented on Novell in Anchorage, Apple-Talk in Fairbanks, and Lantastic in Kenai. These three heterogeneous networks do not talk to each other. E-mail software has been purchased but not yet installed. Development has taken place on a case management system using the FoxPro data base.

d. Computer Project (Memorandum, January 28, 1993, from Blair McCune, Assistant Public Defender, to Brian Duncan, Department of Administration)

This report focuses on case management development progress and plans. The report describes a "conflicts system" noting that it will be included later in the case management. Also described is the manual "index card" system used for case management in Anchorage, with a view toward defining data elements needed for case management.

Appendix B

Operational Structure and Functions of DIS

A. Computer Services

The DIS computer services section supports the operation of data communication and computing resources for the executive and legislative branches of state government. The computer services section designs, installs, operates, and maintains all the equipment and software for its two major data centers[1] and a data communications network connecting the centers with communities throughout the state.[2] It also provides technical support and plans for future use of the data network and data centers. The Section divides into five units: data base services, network services, operations, technical services, and data control.

1. Data Control.

Data Control is responsible for input and output distribution; tape library maintenance; data entry assistance; and job production scheduling for computer operations.

2. Network Services

Network Services manages the data network (SNA and wide area network) facilities. Its duties include resolving problems, modifying or expanding the network, and monitoring the network to ensure reliable and consistent standards for network performance.

Network Services also maintains or coordinates maintenance of the data network facilities, including installing and maintaining customer-owned equipment at the

[1] Two mainframe hosts are the hearts of the data centers: an Amdahl 5995-700A at the Anchorage Data Center and an Amdahl 5995-1400A computer at the Juneau Data Center. Both computers use the MVS operating system.

[2] Approximately twenty-four agencies use over 200 applications on the mainframe computers located in Juneau and Anchorage.

customer's request. Network Services, with the assistance of Technical Services and the Telecommunications Services section, also plans and designs the data network, including network protocols, and the logical and physical connection of facilities.

3. Operations

Operations maintains the physical operations environment; starting and maintaining operation of the central processing units (CPU's) and their operating systems; scheduling hardware and software maintenance; maintaining on-line system schedules; and running batch production and test applications. They also stock paper and special forms; and run printers and associated off-line equipment such as bursters, check signers, and decollators. Operations also distributes all material printed at the data centers.

4. Technical Services

Technical Services installs and maintains operating and systems software needed to run the mainframe computers and the data network. The data network includes seven minicomputers owned and operated by other agencies. Technical Services also solves problems in system software that customers identify. Problems with applications software, however, are the responsibility of agency data processing personnel. Information Center personnel in Customer Services provide application support.

5. Data Base Services

Data Base Services operates statewide data bases, such as the Marine Highways Reservation System (MHRS), the Alaska Statewide Accounting System (AKSAS), and the Alaska Public Safety Information System (APSIN). This group monitors the performance of data bases, maintains security controls, installs upgrades, and solves problems with the data base software.

B. Customer Services and Administration

This section's primary functions include policy development and planning, fiscal and administrative support, customer services (including applications development, programming assistance, data security, and microcomputer assistance) and external relations. Customer Services and Administration is divided into five units: agency support services, fiscal and administrative support, data security, customer support, and information systems planning.

1. Agency Support Services

The Agency Support Services unit assists customers with programming, maintenance, analysis, and design of a variety of mainframe and microcomputer products and systems.

2. Fiscal and Administrative Support

This unit provides the administrative support needed for day-to-day operation of the division. Staff assist the Information Systems Committee (ISC) and the Information Systems Project Review Committee; notify customers of data center activity through on-line notices and monthly customer meetings; and provide clerical support, such as processing mail, filing, photocopying, and answering telephones. Staff also coordinate system changes to the mainframe and help conduct weekly meetings to review these changes.

This unit also maintains accounts payable and accounts receivable for the division. Staff act as supply officers, maintaining the property inventory system; and as purchasing officers, preparing purchasing documents, assisting in the preparation of RFP's, and assuring adherence to purchasing regulations. In addition, this unit prepares and maintains the federal cost accounting system, monitors job accounting for the mainframe services, and prepares DIS budget documents.

This unit also creates and disseminates division publications. These include a bi-monthly newsletter promoting relations between the division and its general customers; a DIS Guide to Data Center and Telecommunications Services; and several informational pamphlets and brochures.

3. Data Security

The data centers use a security software product called ACF/2 to assist agencies with data security. In addition, the security administrator helps agencies determine their security requirements and then helps implement access controls.

4. Customer Support

The Customer Support unit is the focal point for all service delivery from DIS. Agencies contact this unit when they desire a new service or have questions about service policies or billings. The unit includes customer service representatives and customer service specialists, who maintain computer accounts for customers, help with password problems, document and track requests for service, document and resolve technical questions or problems concerning DIS services and products, answer policy and billing questions associated with DIS services, identify customer service requirements and expectations, maintain service-level agreements with customer agencies, support and manage changes to DIS services and procedures, measure and report service quality provided to customers, and provide state mainframe-related training opportunities. Staff also coordinates on-line and classroom training for many mainframe-related programs and applications.

5. Information Systems Planning

This group develops policy recommendations for short and long-term plans, and drafts statewide standards for the state's information systems and telecommunications activities.

C. Telecommunications Services.

This section designs, operates, and maintains the telecommunication systems used by state agencies. Included are radio, data, telephone, and alarm circuits; radar repairs for state vessels; mobile/portable radio systems; teleconferencing; and a statewide paging network. Some of these systems are diagrammed on Figures B-1, B-2, and B-3 at the end of this appendix. Telecommunications staff procure and maintain all required FCC licenses. Telecommunications Services also provides direct service to rural Alaska through operation of the Rural Alaska Television Network (RATNet) and remote TV site repairs. Four subunits are included in this unit: engineering, maintenance, tape delay center, and telephone procurement.

1. Engineering

The engineering section plans and implements a statewide voice and data communications network, including long-range requirements, new products and software releases, and upgrades for user agencies as required. The engineering staff also coordinates installation of communications networks statewide, reviews user agencies' usage of networks, and recommends more effective use of networks.

2. Maintenance

The maintenance shops located in Juneau, Anchorage, Fairbanks, Glennallen, and Soldotna provide electronic maintenance services to the client agencies served by Telecommunications Services.

3. Tape Delay Center

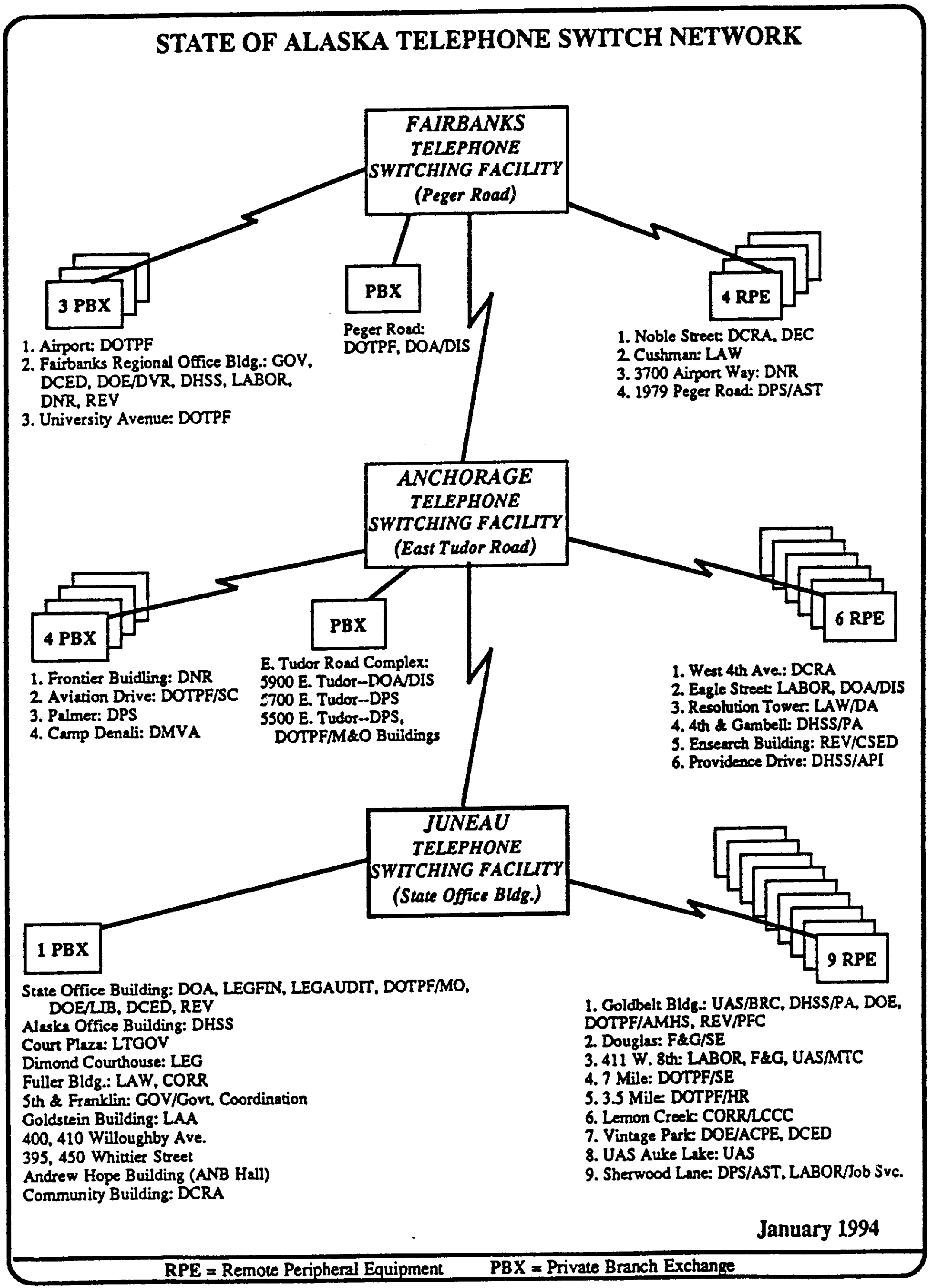
The tape delay center is staffed 18.5 hours per day by technicians who prepare programming for broadcast and monitor and ensure its delivery over the RATNet. The project assistant facilitates RATNet Council meetings, coordinates programming with sources, creates and distributes the program schedule, and also acts as a liaison between viewers and the RATNet Council.

4. Telephone Procurement

This unit competitively solicits proposals for office telephone and teleconferencing equipment for state agencies that need new systems, moves, or changes. This requires planning, engineering, compliance with state procurement codes, and a great deal of interaction with both client agencies and the telephone vendor community statewide.

FIGURE B-1

INFORMATION SYSTEMS DIAGRAMS


STATE OF ALASKA TELEPHONE SWITCH NETWORK
FAIRBANKS TELEPHONE SWITCHING FACILITY (Peger Road)
3 PBX
PBX
4 RPE
ANCHORAGE TELEPHONE SWITCHING FACILITY (East Tudor Road)
4 PBX
PBX
6 RPE
JUNEAU TELEPHONE SWITCHING FACILITY (State Office Bldg.)
1 PBX
9 RPE

1. Airport: DOTPF
2. Fairbanks Regional Office Bldg.: GOV, DCED, DOE/DVR, DHSS, LABOR, DNR, REV
3. University Avenue: DOTPF

Peger Road:
DOTPF, DOA/DIS

1. Noble Street: DCRA, DEC
2. Cushman: LAW
3. 3700 Airport Way: DNR
4. 1979 Peger Road: DPS/AST

1. Frontier Buidling: DNR
2. Aviation Drive: DOTPF/SC
3. Palmer: DPS
4. Camp Denali: DMVA

E. Tudor Road Complex:
5900 E. Tudor--DOA/DIS
5700 E. Tudor--DPS
5500 E. Tudor--DPS, DOTPF/M&O Buildings

1. West 4th Ave.: DCRA
2. Eagle Street: LABOR, DOA/DIS
3. Resolution Tower: LAW/DA
4. 4th & Gambell: DHSS/PA
5. Ensearch Building: REV/CSED
6. Providence Drive: DHSS/API

State Office Building: DOA, LEGFIN, LEGAUDIT, DOTPF/MO, DOE/LIB, DCED, REV
Alaska Office Building: DHSS
Court Plaza: LTGOV
Dimond Courthouse: LEG
Fuller Bldg.: LAW, CORR
5th & Franklin: GOV/Govt. Coordination
Goldstein Building: LAA
400, 410 Willoughby Ave.
395, 450 Whittier Street
Andrew Hope Building (ANB Hall)
Community Building: DCRA

1. Goldbelt Bldg.: UAS/BRC, DHSS/PA, DOE, DOTPF/AMHS, REV/PFC
2. Douglas: F&G/SE
3. 411 W. 8th: LABOR, F&G, UAS/MTC
4. 7 Mile: DOTPF/SE
5. 3.5 Mile: DOTPF/HR
6. Lemon Creek: CORR/LCCC
7. Vintage Park: DOE/ACPE, DCED
8. UAS Auke Lake: UAS
9. Sherwood Lane: DPS/AST, LABOR/Job Svc.

January 1994

RPE = Remote Peripheral Equipment PBX = Private Branch Exchange

Appendix F.2

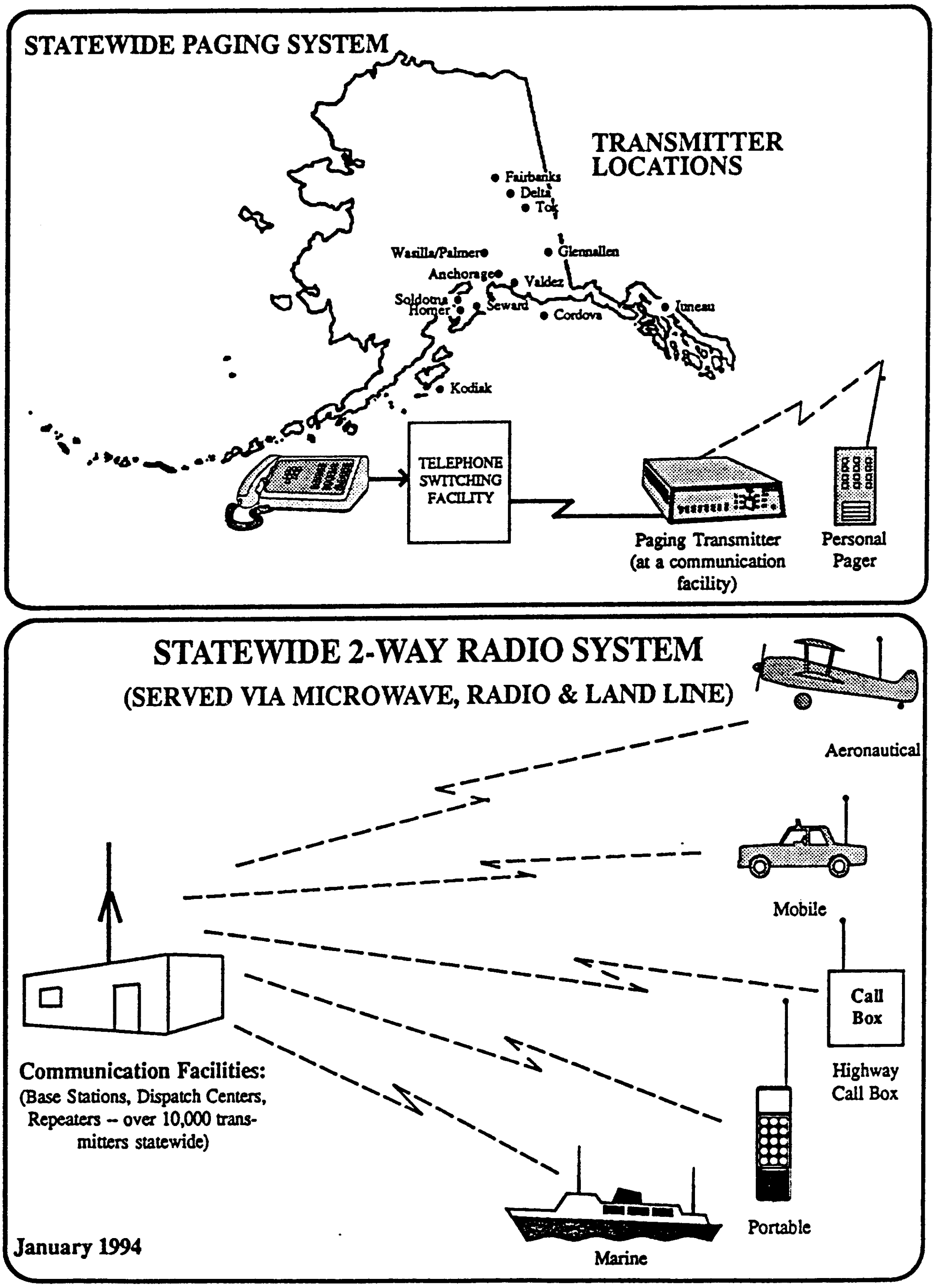
Alaska 1994 Information Management Plan

DRAFT

2/94—19/5/25YSTEMS.PM5/2

FIGURE B-2

INFORMATION SYSTEMS DIAGRAMS

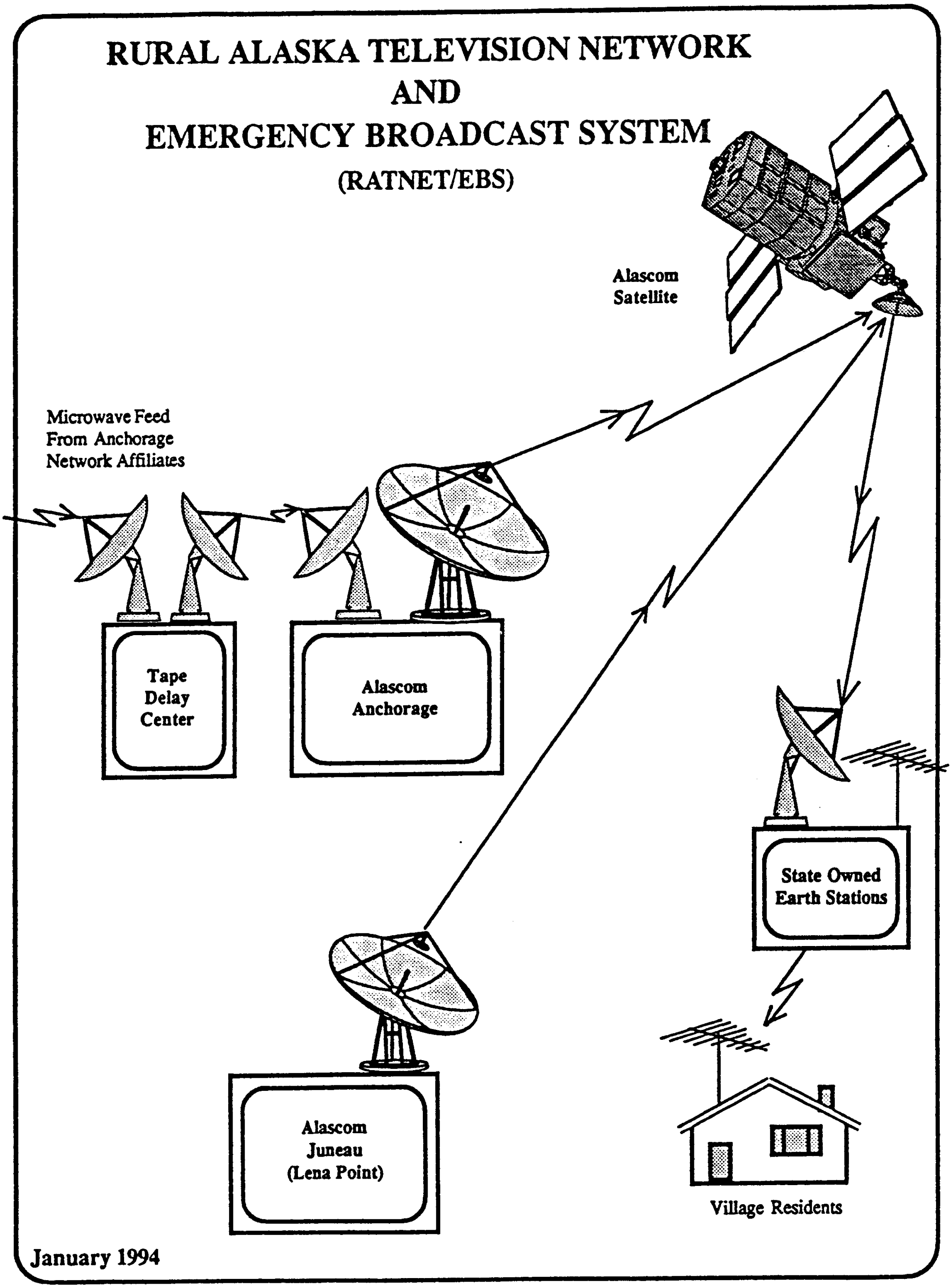

STATEWIDE PAGING SYSTEM
TRANSMITTER LOCATIONS
Fairbanks
Delta
Tok
Glennallen
Wasilla/Palmer
Anchorage
Valdez
Soldotna
Homer
Seward
Cordova
Juneau
Kodiak
TELEPHONE SWITCHING FACILITY
Paging Transmitter (at a communication facility)
Personal Pager
STATEWIDE 2-WAY RADIO SYSTEM
(SERVED VIA MICROWAVE, RADIO & LAND LINE)
Aeronautical
Mobile
Call Box
Highway Call Box
Portable
Marine
Communication Facilities:
(Base Stations, Dispatch Centers, Repeaters – over 10,000 transmitters statewide)
January 1994

Alaska 1994 Information Management Plan **Appendix F3**

19/6/2SYSTEMS.PM5/3—2/94 DRAFT

FIGURE B-3

INFORMATION SYSTEMS DIAGRAMS


RURAL ALASKA TELEVISION NETWORK
AND
EMERGENCY BROADCAST SYSTEM
(RATNET/EBS)
Alascom Satellite
Microwave Feed From Anchorage Network Affiliates
Tape Delay Center
Alascom Anchorage
State Owned Earth Stations
Alascom Juneau (Lena Point)
Village Residents
January 1994

Appendix C

Commentary on APSIN Fingerprint Legislation (HB442 and SB276)

The governor has introduced legislation to revise Alaska's statutes that govern how agencies acquire, verify, use, and disseminate criminal justice information. The Department of Law has commented extensively on the companion bills. The commentary included here focuses primarily on the parts of the bills that will affect integration of the criminal justice computer information systems, and operation of the CCH (criminal case history). The commentary also analyzes parts of the legislation that tie Alaska to federal laws such as the Brady Bill, the Child Protection Act, the FBI Interstate Identification Index (III), the FBI Integrated Automated Fingerprint Identification System (IAFIS), and NCIC 2000.

The proposed legislation supports the strategic plan for integrating Alaska criminal justice information systems by including:

* Mandatory reporting of criminal justice information
* Adoption of a unique case tracking number;
* Monitoring of arrest and disposition reporting;
* Mandatory fingerprinting of defendants;
* Timely reporting of fingerprints;
* Standardized data entry;
* Regular audits, training, and data security.

A. AS 12.62.110: Promulgation of regulations governing the repository

The statute requires the Commissioner of Public Safety to promulgate regulations governing the central repository. This provision is essential to ensure authority for the specification of data elements, and reporting responsibilities for arrest and disposition reporting. Because DPS must maintain the criminal record, it should have the ability to enforce statutory requirements for reporting information to the repository. For example, DPS should lead the effort to define elements in the criminal history record, and to manage the data that comprise the record. The Commissioner also can ensure, through regulations, that contributing agencies maintain records sufficient to meet the needs of the audits required by the statute.

B. AS 12.62.100 -- Criminal Justice Information Board

Subsection (a) establishes the Criminal Justice Information Board in the Department of Public Safety. We recommend that the Board's responsibilities include the oversight and guidance of information technology projects related to the coordination and integration of criminal justice information systems. The Board would review proposals for developing new information systems and applications that affect the criminal history record, and would comment on the proposal's compliance with the state's overall plan for integrating criminal justice information. The Board would advise, without authority to approve or disapprove proposals. Endorsement by the Board will assure the legislature and other criminal justice agencies that the proposal would benefit the criminal justice system as a whole. We also recommend that the Judicial Council be added to the Board (and understand this change already has been made in both versions of the legislation).

C. AS 12.62.120--150 -- Reporting Fingerprints

We concur with the provision that limits fingerprinting and reporting requirements to felonies until July 1, 1996. We recognize the costs and administrative problems in requiring that all misdemeanants be fingerprinted, and the convictions and fingerprints reported. We recommend that the state consider requiring mandatory fingerprinting and reporting only for felonies and serious misdemeanors.

Alaska, like many states, issues citations in lieu of arrest for certain misdemeanors. Also, some felony defendants are required to appear in court by means of a summons rather than arrest. In many instances, the offenders who are cited or summonsed are not fingerprinted, so the association of the arrest and case disposition with the specific defendant is not supported by the positive identification of unique fingerprints. The FBI Voluntary Reporting Standards and the BJA Guidance for improving Criminal Record Information call for a fingerprint record to support each arrest event. A fingerprint record also must support criminal history records provided to other states through the FBI III. If non-fingerprint-supported records mingle in the CCH data base with fingerprint-supported records, the state must be able to separate them out, and assure that they are not disseminated. We understand that the state now uses a status flag to show which records are supported by fingerprints, and will provide a means of separating the two types of records.

D. AS 12.62.120 -- Fingerprinting at Stages of the Criminal Justice Process

Subsections (a), (b), and (c) set requirements for taking fingerprints at different points in a case. Arresting officers must take fingerprints. Courts must order fingerprinting for a person charged with a crime but not arrested (i.e., summonsed or cited), or convicted but not previously fingerprinted. The Department of Corrections must fingerprint any person committed to a correctional institution. Subsection (d) sets a limit of five days to send fingerprints to the central repository, and subsection (e) requires the repository to confirm the defendant's identity through fingerprint comparison and to inform the agency that took the prints if the defendant appears to be using an alias.

We believe that these requirements for fingerprints will greatly improve the integrity of the criminal history records and result in much higher-quality data. We recommend that the five-day time limit for forwarding fingerprints be shortened to one day. A shorter period is reasonable in the great majority of circumstances and is a better goal.

E. AS 12.62.130 -- Authority of the Commissioner

This section gives the commissioner authority to specify the "reportable events" needed to construct complete and useful criminal history records, and permits the commissioner to specify which agencies will report each event. Over time, the commissioner will articulate an expanded set of data elements for the criminal history record, maximizing its usefulness to each agency. We recommend that, once the CCH is electronically connected to each of the reporting agencies, data be downloaded daily, in batch mode rather than real time, during non-peak-use hours.

F. AS 12.62.160 -- Procedures to Ensure Data Quality and Security

This section calls for manual and automated procedures to ensure data quality and the security of the records in the CCH. It includes edit checks and means of linking arrests and dispositions. The section recognizes the practical problems of data already in the system that cannot be validated for data quality or linked to other data elements. We recommend here that DPS set up edit checks and validation criteria that eventually will permit automated name searches, and the electronic submission of disposition data without manual intervention.

G. AS 12.62.190 -- Sealing Criminal History Records

This section permits the court to seal part or all of a criminal history record. DPS might consider electronic sealing, by one of two methods. The first method would involve reading the sealed portion or entire record to electronic media, and separately storing the medium in a secure place. The second would involve "electronically masking" the specific information, leaving it on the system, to be viewed only within DPS with special password control. Either method would permit DPS to unseal the record and put it back "online" should the court so order.

H. AS 12.62.900 -- Dissemination of Criminal History Record Information

The CCH should automatically screen the types of information available to different users. Criminal justice agencies normally will be cleared to view arrest and conviction information. Other agencies and the public generally will be allowed to see only conviction information.

Appendix D

Proposed Open System Standards for Alaska

A. Server Hardware Specifications

Specific server hardware standards should, as a minimum, include:

- Highly scalable hardware, which will allow for binary program compatibility, across the vendors' hardware platforms. A multi-processor system capability would be desirable, but this upgrade option may depend upon the data base software employed.

- Demonstrable interoperability in a multi-vendor, networked environment that includes mainframes.

- Capabilities for Ethernet (IEEE 802.3) and Fiber Distributed Digital Interface (FDDI) network conductivity. Ethernet connections can provide up to 10 megabytes per second transfer rates, and FDDI provides 100 megabytes per second transfer rates.

- Support of multiple Small Computer Systems Interconnect (SCSI), Fast Wide SCSI (SCSI-FWS), and SCSI-2 Interfaces. These standards allow connections among fixed media disks, optical removable drives, tape drives, and media changers such as HP optical jukeboxes. The SCSI-2 further allows two host computers to connect to the same bus, and share devices. The Fast Wide SCSI has a very high transfer rate of about 10 to 20 MBytes, which will be particularly useful with RAID arrays.

- The capability to support a minimum of 64 MBytes of main memory, expandable to two GBytes, with hardware upgrades.

- The support of a minimum of 10 GBytes of SCSI disk storage, expandable to 250 GBytes, with hardware upgrades. Hardware implementations of Redundant Array of Inexpensive Disk (RAID), levels 1 through 5, are desirable. RAID provides a level of fault tolerance, high-speed access via striping, and volume shadowing, by selecting the level needed for an application.

B. Server Software Specifications

Specific server software standards should, as a minimum, include:

- Unix System V Revision 4 (SVR4), compliant Operating System adhering to the *System V Interface Document (SVID), issue 3 Application Program Interface.*(API). Unix SVR4 is the product of Unix Systems Laboratories (USL). For a vendor to comply with this SVR4, it must pass a set of rigid tests by USL. This de-facto standard is published as the System V Interface Document, issue 3 API.

- Compliance with the IEEE's *POSIX 1003.1 Operating Systems Interface Standard.* Most systems, including System V, have not used the same set of rules for making system calls to the operating system. This caused major problems with porting source code from one Unix system to another. IEEE Standard 1003.1-1988 defines a standard operating system interface and environment based on the Unix Operating System documentation, to provide for the portability of application software at the source-code level, between computer systems from multiple vendors.

- Full support for the Transport Control Protocol (TCP) and the Internet Protocol (IP), and the standard support services such as ftp, ftpd, telnet, telnetd, mail, etc.

- Serial Line Internet Protocol (SLIP) and Compressed SLIP (CSLIP) support services. This will allow sites not connected to the dedicated statewide Internet to have access to the same services, but with potentially slower on-demand phone lines.

- Network File System (NFS) server and client services.

- The provision of the University of California at Berkeley's *"r"* command extensions, such as rlogin, rsh, rshd, rexec, rcp client and server programs. These programs let users connect to any machine on the network with interactive access, or to execute remote commands.

- Compliance with XPG3.

- Support for X11 Revision 5 (X11R5) and the Motif open desktop. The X11 client running on a host machine allows X-terminals or PC's with X11 server software to create windows into remote machines to access information, tools, or for interactive use. This is similar to the Microsoft product MC/Windows 3.1, but designed with a network in mind.

- Local and remote laser and dot matrix printer service support. This will provide capabilities of printing on any printer connected to the network.

- Supports software that provides IBM SNA access, including IBM 3270 terminal emulation for ASCII or X-terminals.

- Can do a remote network backup of distributed client departmental servers and workstations.

- Support of relational data base with SQL query interface, and perform as a back-end network server, such as ADABAS, ORACLE, Sybase, or Ingress.

- Software driver support for RAID levels 1 through 5. RAID technology is discussed in more detail in the Server Hardware Specifications.

C. Desired Server Software Services

Desirable server software features include:

- A hierarchical file system, with automated tape or optical disk robotics support that follows the IEEE Mass Storage Reference Model, Version 5.

- Support for Distributed Computer Environment (DCE) and Distributed Management Environment (DME) software, such as TUXEDO from Unix Systems Labs. TUXEDO is a transaction processing monitor that claims to be 100% compatible with IBM's CICS applications, and offers the same type of functionality. Also the capability for remote procedure calls (RPC), should be provided.

- Capable of operating in a network clustered environment. This would eliminate the need for expensive hardware upgrades. New processors could be added to the cluster to help process the distributed system load.

D. Client Hardware Specifications

Specific client hardware standards should, as a minimum, include:

- Low-end workstation scalable to a departmental server without major hardware upgrades.

- Compatible interoperability with the central server system.

- Support of a single IEEE 802.3 Ethernet network interface.

- Supporting synchronous terminal access for both local and dial-in users. However, this type of service is better left to terminal servers, attached to the network.

- Support of 20 to 60 concurrent X-terminal or PC sessions. This does not mean 20 to 60 users; a single user may have one or more sessions active at the same time, with each accessing different applications.

- Support of multiple Small Computer Systems Interconnect (SCSI), Fast Wide SCSI (SCSI-FWS), and SCSI-2 Interfaces.

- Support of up to 5 GBytes of SCSI disk storage.

- Support of up to 64 MBytes of main memory.

E. Client Software Specifications

Specific client software standards should, as a minimum, include:

- Unix System V Rev. 4 compliant Operating System.
- Compliance with the POSIX 1003.1 Operating Systems interface standards.
- Full support for the Transport Control Protocol (TCP) and the Internet Protocol (IP) and the standard support services.
- Serial Line Internet Protocol (SLIP) and Compressed SLIP (CSLIP) support services.
- Network File System (NFS) server and client services.
- The provision of the University of California at Berkeley's *"r"* command extensions, such as rlogin, rsh, rshd, rexec, rcp client and server programs.
- Compliance with XPG3.
- X11 Rev. 5 & Motif open desktop support.
- Support of local and remote laser and dot matrix printer service. This will permit printing on any printer connected to the network.
- Support of software that provides IBM SNA access, including IBM 3270 terminal emulation for ASCII or X-terminals.
- Capability of performing remote network backup of distributed client departmental servers and workstations.

- Support of front-end client software to access back-end data base systems.

- Support of relational data base with SQL query interface, perform as a back-end network server, such as ADABAS, ORACLE, Sybase, or Ingress.

F. Desired Client Software Specifications

Desirable client software standards include:

- Support for DCE and DME software, such as TUXEDO from Unix Systems Labs.

- Support remote backup operations to the main server, as a client.

G. Information Access Considerations

Most of the information provided in this section addresses points that the state should consider when developing a distributed system connected via a network.

- Provide TCP/IP network access to information within the data base.

- The back-end server should provide multi-processor support for the central server or servers. This is not as important for data bases residing on small departmental servers.

- The back-end server should support several types of processors, including Sparc, RISC, Mips, Alpha, Intel, PowerPC, just to name a few of the major ones.

- The back-end servers must support stored procedures. This will reduce much of the network traffic and increase the performance of the application from minutes and hours to seconds.

- Careful selection of the back-end server should allow for a diverse selection of front-end clients. Do not select a back-end server that locks you into a proprietary front-end client or limits your software vendor solutions.