THE SHARING OF CRIMINAL INVESTIGATION INFORMATION AMONG CALIFORNIA LAW ENFORCEMENT AGENCIES BY THE YEAR 2000

by

THOMAS H. SIMMS
COMMAND COLLEGE CLASS XII
PEACE OFFICER STANDARDS AND TRAINING

SACRAMENTO, CALIFORNIA
July - 1991

This Command College Independent Study Project is a FUTURES study of a particular emerging issue in law enforcement. Its purpose is NOT to predict the future, but rather to project a number of possible scenarios for strategic planning consideration.

Defining the future differs from analyzing the past because the future has not yet happened. In this project, useful alternatives have been formulated systematically so that the planner can respond to a range of possible future environments.

Managing the future means influencing the future--creating it, constraining it, adapting to it. A futures study points the way.

The views and conclusions expressed in this Command College project are those of the author and are not necessarily those of the Commission on Peace Officer Standards and Training (POST).

INTRODUCTION
A background for the future

FUTURES STUDY
What problems will California law enforcement agencies face when sharing criminal investigation information by the year 2000?

STRATEGIC MANAGEMENT
A plan for managing information systems technology by California law enforcement administrators.

TRANSITION MANAGEMENT
Managing the transition to integrated regional information systems.

CONCLUSIONS, RECOMMENDATIONS, AND FUTURE IMPLICATIONS
The next ten years - and beyond.

THE SHARING OF CRIMINAL INVESTIGATION INFORMATION AMONG CALIFORNIA LAW ENFORCEMENT AGENCIES BY THE YEAR 2000

by

THOMAS H. SIMMS
COMMAND COLLEGE CLASS XII
PEACE OFFICER STANDARDS AND TRAINING (POST)
SACRAMENTO, CALIFORNIA
1991

Executive Summary

California is now called home by nearly 30 million Americans and annually reports more crime than any state in the union. More than 500 law enforcement agencies provide police services in the cities and unincorporated areas, ranging in size from one-member agencies to those with more than 8,000 sworn officers.

Despite the leadership role California's high-tech industry has played throughout the world, California law enforcement is surprisingly low-tech when it comes to the automated sharing of criminal information. Few agencies share even the most basic information, such as names of persons suspected of committing crimes.

The reasons for this situation are many: lack of standards for the identification of individuals; lack of standards for the gathering, storing and releasing information; lack of funding; an unwillingness or inability of agencies to change; and the lack of an integrated state-wide master plan.

A futures forecasting process focused upon the issue, "What problems will California law enforcement agencies face when sharing criminal investigation information by the year 2000?" The sub-issues were police agency resistance to changing their information systems and the ability of police agencies to fund information systems. The results of this group process showed a great deal of uncertainty regarding the future of law enforcement funding in general, and specifically funding for computer systems. The group concluded that two elements are essential to a successful system: state-funding and a better system for identifying individuals.

A strategic management plan is presented which outlines the process by which regional information systems can be linked together to provide a state-wide information system. It identifies the California Commission on Peace Officer Standards and Training as providing the initial leadership in studying the problem and identifying solutions. Further, it proposes a Task Force chaired by the Attorney General, with membership from California state Chiefs and Sheriffs, the Legislature and the Governor.

The formation of several state agencies is necessary, including a Technical Standards Committee and a Law Enforcement Technology Procurement Agency. The study also identifies several important state policies and laws, including: a mandate that agencies receiving state funding share information and adhere to standards, funding for regional information systems, and new laws to protect the privacy of this information.

Many of the funding concerns addressed in the futures study can be addressed by eliminating the proliferation of computer systems which serve a narrow range of interests, by establishing standards and by establishing a state agency to evaluate and procure technology. Support for the funding of police computer systems will be easier to obtain for a well thought out plan, as opposed to the fragmented and ineffective systems presently found.

Police reluctance to change existing systems will be overcome by: 1) establishing an integrated plan which will provide maximum sharing of information, 2) providing funding for networking based upon participation, and 3) mandated participation for those receiving funding.

Several other areas of possible future study were identified, including the privatization of information systems, the commercialization of law enforcement information, and the right of individuals to privacy versus the right of others to access government information.

CONTENTS

ILLUSTRATIONS

TABLES

THE SHARING OF CRIMINAL INVESTIGATION INFORMATION AMONG CALIFORNIA LAW ENFORCEMENT AGENCIES BY THE YEAR 2000

INTRODUCTION

California law enforcement has not taken full advantage of advances in information systems technology. Most California agencies have manual record keeping systems and those with automated systems generally do not share the information with other agencies.

The Setting:

California is the most populous state in the nation with the largest number of reported crimes. It also has more high-tech industries than any other state. However, despite this high crime rate and the availability to high technology, there has been little effort by law enforcement agencies to share information through the linking of automated information systems.

The total number of police agencies within the state is staggering. In 1988 the California Commission on Peace Officer Standards and Training (POST) reported that 563 agencies were members of their certification program. This number does not include Federal or private police agencies operating within the state.

Will California take a leadership role and improve the automated sharing of information in the future?

The Need for Networked Information Systems:

- Lee Brown, President of IACP (International Association of Chiefs of Police), recently termed a Bush administration plan to allow "point-of-sale" checks of prospective handgun purchasers unworkable. Citing the need for a complete criminal history and a

national index, Brown stated, "..it could take more than a decade to implement a computerized system .." [1] Without networked information systems, checks of potential handgun purchasers will continue to result in incomplete and untimely information.

- In April 1990 the California Department of Justice conducted a survey of all state law enforcement agencies to determine their need for an expansion of automated information systems. The survey concluded that there is little automated information sharing taking place between counties (2 of 28 responses) and fewer than 3% have automated their notification process. **Respondents stated that personal contact is the nearly exclusive means by which they share information.** They further concluded that the lack of an automated system hampers the investigation of crimes (99%), and officer safety is compromised (79%).

- The California Identification System (Cal-ID) automated the state's fingerprint identification process and resulted in spectacular crime clearance data. Agencies throughout the state are linked together in a system which uses computers to identify suspects from latent prints left at crime scenes. The Sacramento Police Department, serving a population of 340,483, reported 200 matches of latent fingerprints with suspects during the period July 1987-May 1988.

Areas of Potential Concern:

- **Security:** The security of networked systems can be violated, regardless of

---

[1] San Francisco Chronicle, April 14, 1991, p 2. *Police Group Says Gun Plan Won't Work*

precautions taken to protect them. United States military computer systems were recently the object of computer "hackers" operating from Holland. Members of the Dutch group used telephone lines to access the sensitive files maintained by the government. Investigators working on the case quoted members of the group as stating, "... that they could enter computers via international data networks with impunity." [2]

- **Civil Rights:** Lawrence Tribe, professor of constitutional law at Harvard, recently called for a constitutional amendment to protect the public from computerized intrusions into their private lives. In declaring the need for this protection, Professor Tribe stated, "Constitutional principles should not vary with accidents of technology." [3] European nations are moving much faster than the United States in ensuring individual privacy in an increasing technological age. The European Economic Community recently enacted strict guidelines regarding the transfer of personal information between computer systems. An article in the New York Times stated, "They are intended both to make privacy laws uniform ... and to restrict the flow of information to nations without stringent privacy laws." [4]

- **Vulnerability to Disruption** A severed telephone cable brought the entire New York stock market to its knees. Despite redundant systems, a maintenance crew digging in

---

[2] San Francisco Chronicle, p. A3, May 8, 1991. *Dutch Hackers Brag of US Trespasses"*

[3] ComputerWorld, p 34, April 1, 1991. *Constitutional Scholar Calls for High-Tech Amendment*

[4] San Francisco Chronicle, April 11, 1991 p C2. *Europe Restricts Flow of Computerized Data*

the streets of the nation's largest city shut down one of the most sophisticated networks in the world. A wall street expert was quoted as saying, "The loss of the cable underlined how society's reliance on new technology carries a risk because it concentrates so much information in one place." [5]

- **Lack of Standards.** The large number of police agencies in California has spawned an almost equally large number of software systems. Each police agency has the discretion of developing its own police reports and defining the names of the various entries or "fields" contained in the reports. This leads to a confusing array of terms used to express the same idea. For example, does one refer to a person as a "suspect, a "responsible," or a "perpetrator." This lack of standardization can be compared to the difficulties faced by countries in the European Economic Community. With different languages and different currency, their ability to carry on commerce between countries has been greatly constrained.

Equally as significant, the computer hardware industry lacks standards. There have been recent efforts to develop standards, however these efforts seem to be directed by consortiums of vendors attempting to carve out personal niches in the hardware market. One of the strongest moves for standardization was recently made in New York City. Commenting on this latest attempt at industry standardization, John Dunkle, an analyst with WorkGroup Technologies stated, "It's another consortium that is going to tout the latest and best

---

[5] San Francisco Chronicle, p 1, January 6, 1991. *Severed AT&T Cable Causes Big Disruption in NY*

technology to usurp the other consortiums." [6]

- **The automated sharing of information between agencies is the rare exception, rather than the rule in California.** According to a recent survey conducted by the California Department of Justice, approximately 70% of California law enforcement agencies do not automate their record systems. Of those who do, few share this information with other agencies through automated means. The most commonly used crime fighting technology used by these departments is the telephone.

- **The development of California law enforcement information systems is driven by vendors, not by the law enforcement community.** The lack of networked systems and the lack of standards for data exchange has resulted in a very confusing and generally unattractive marketplace for hardware and software developers. With the average agency size of 20 officers, only the largest and wealthiest agencies can purchase customized systems. This forces the majority of law enforcement agencies to purchase whatever is available from the vendors.

---

[6] San Francisco Chronicle, p C7, April 8, 1991. *Computer Firms to Lobby on Compatibility*

SECTION ONE: DEFINING THE FUTURE

WHAT PROBLEMS WILL CALIFORNIA LAW ENFORCEMENT AGENCIES FACE WHEN SHARING CRIMINAL INVESTIGATION INFORMATION BY THE YEAR 2000?

THE SHARING OF CRIMINAL INVESTIGATION INFORMATION AMONG CALIFORNIA LAW ENFORCEMENT AGENCIES BY THE YEAR 2000

Part one of this study will focus on defining the future of automated information sharing by law enforcement agencies in the state of California. Before it is possible to define the future, one must focus on the issue and most important sub-issues to be studied.

OVERVIEW AND METHODOLOGY

Extensive interviews were conducted with professionals in the field of automated information sharing. These interviews included a broad spectrum of individuals, including: law enforcement administrators who were instrumental in developing networked systems, agencies currently developing systems, state government officials, computer system developers and computer system vendors. A literature search was conducted using the resources of several large agencies, including the National Criminal Justice Reference Service.

The interviews and the literature search revealed information which differed greatly. Generally, the literature discussed success stories in glowing terms while the interviews chronicled tales of frustration and adversity. This result was unexpected, but made sense. Most people don't write about their failures, only their successes.

STRUCTURING THE ISSUE AND SUB-ISSUES

The literature search and interviews provided insight into what has been done and what law enforcement is currently doing. However, there was little information available which discussed the future of information sharing. To gain a perspective of what the future might be, several processes were employed. Relying on personal interviews a "Futures Wheel" was generated to identify the most important areas related to this field. Other sub-issues were identified through a review of the literature. Both sources assisted in focusing on the issue and the most important related sub-issues.

In narrowing the related sub-issues, two main criteria for selection were used. First, the sub-issue had to be one which was critically important to the issue. This eliminated trivial matters from consideration. Second, the sub-issue had to be one which could be influenced by policies. If it was a sub-issue outside the control or influence of law enforcement executives it was felt to be unworthy of further consideration. This process eliminated many other sub-issues which were considered by the researcher.

The focus of this report has intentionally been drawn away from technical and directed towards topics which reflect attitudinal issues and policy alternatives. An assumption has been made, based upon substantial confirmation in the literature search and expert interviews, that current technology enables us to construct whatever networked information system we might design. Persons interviewed repeatedly stated that the technical problems are much more easily resolved than the people-oriented problems. Though seldom vocalized, attitudes such as "if it wasn't invented here, it can't be any good" are prevalent in

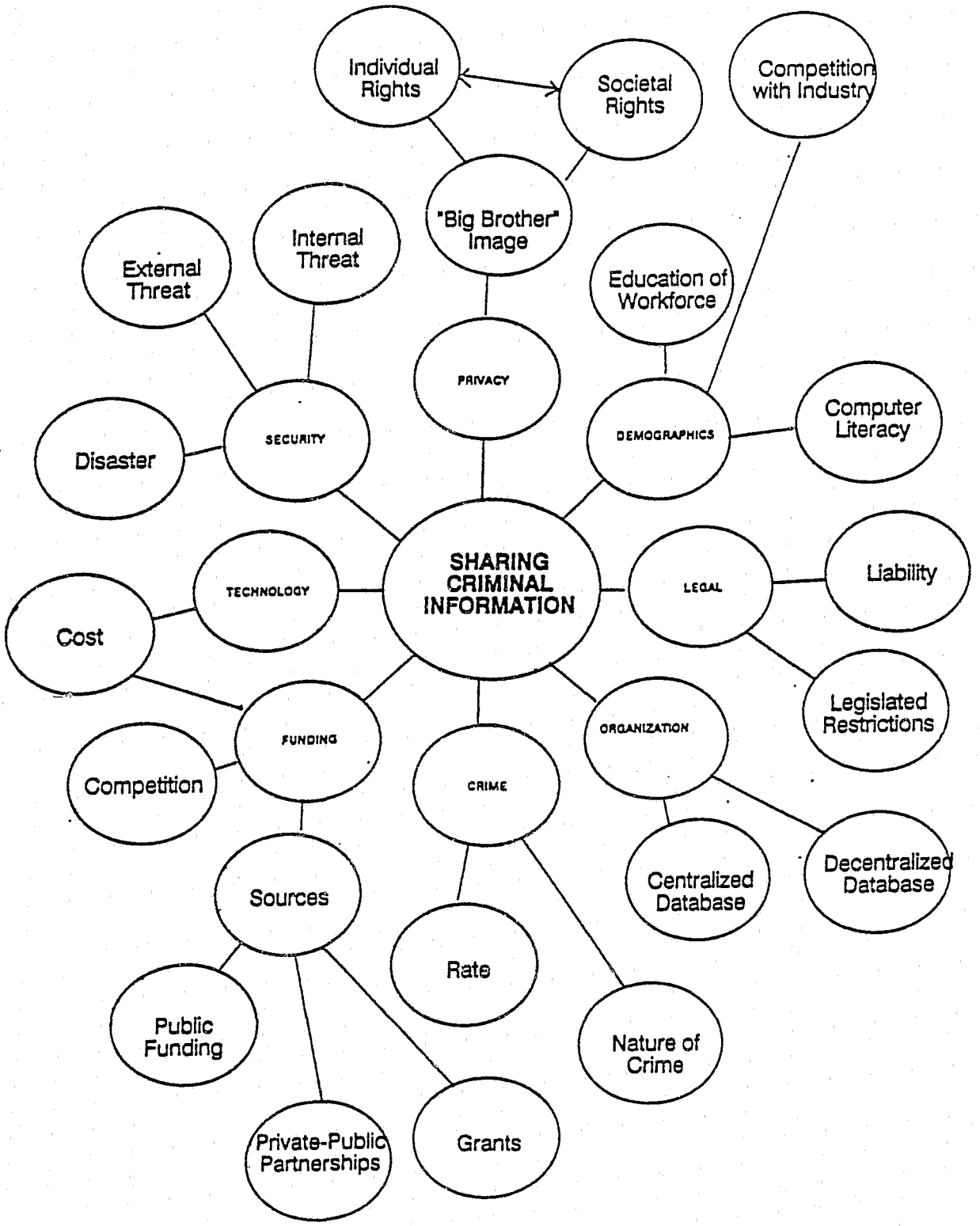
law enforcement.

Issue: *"What problems will California law enforcement agencies face when sharing criminal investigation information by the year 2000?"*

Sub-Issue: *Police agency resistance to changing their information systems.*

Sub-Issue: *Ability of police agencies to fund information systems.*

FUTURES WHEEL



INTERPRETING THE DATA COLLECTED

A forecasting process was conducted using a group of experts in the field. These people represented a wide spectrum of interests related to this field.[7] They were provided with a description of the study and the issues and sub-issues. A listing of candidate trends and events developed from the futures file and literature search were included for their consideration. Using this information as a starting point, the group identified the five most significant trends and the five most significant events. Forecasts were made of each of the trends and events. The following is an analysis of the group findings:

Selected Trends:

Trend-1 Funding for computerization.

The group differed significantly in their forecasts of funding with no consensus being reached. Law enforcement agencies in California have benefitted from both Federal funding and state grants in the development of their systems. However, these grants are becoming increasingly scarce and California now faces its largest budget deficit in history. Even the most optimistic group members felt that funding levels will decline over the next ten years. This opinion is consistent with recent newspaper articles which forecast a $9-11 billion state deficit.

The researcher disagreed with the gloomy projections of the group. There are many

---

[7] See Appendix B for listing of NGT participants.

funding mechanisms available for law enforcement projects. Some of these strategies include bond measures for specific projects, grant funding and supplemental taxation. Combined with the high degree of public support law enforcement generally enjoys, well-developed and cost-effective programs should be well received by elected policy makers.

Trend-2 Public Concern for Privacy

A surprising conclusion of the panel was that the concern for individual privacy will actually decrease in the future. The image of "Big Brother" does not weigh on people's minds the way that it did just a few years ago. This is significant in determining the public's acceptance of automated systems.

Trend-3 Standardized methods for the collection and retention of information.

There was strong agreement that police agencies of the future will have greater standardization of methods for the collection and storage of criminal information. Panel members felt that standardization will be necessary if networking between agencies is to take place.

Trend-4 Public expectation of police role as "service providers."

There was strong disagreement among panel members concerning the future role of police as service providers. They were evenly divided between those who view the police as having a greater role and those who see the police as having a diminishing role. Despite a detailed discussion, there was no resolution to this issue. One possible explanation could be

the difference in outlook between the agencies they represent. For example, a person working for an agency which is well funded and provides a high level of services would assume that the public will expect a continued high level of service. Conversely, a person from an agency which is continually forced to reduce service levels will likely see a decreased service expectation.

Trend-5 The rate of change of technology.

Panel members saw technology changing at an increasing rate. This is consistent with projections made by various publications. However, they also stated that technology should not be changing as fast as it does. The rapid pace of change is impossible for agencies to maintain. It creates pressure to constantly upgrade systems to keep up with the latest developments. This attempt to keep pace with technology takes away from departments ability to perfect their existing systems before launching into new projects.

Selected Events:

Event-1 State mandates a state-wide system and makes funding available.

The more conservative members of the panel felt that there is little chance of a state system being implemented during the next 10 years. However, most panel members assumed that the need to share this information will spawn a system similar to CAL-ID, a statewide latent fingerprint identification system.

Event-2 Court rules that electronically stored information is not admissible in court.

The panel felt that there is little chance that courts will rule against the use of electronically stored information in criminal matters.

Event-3 Legislature passes comprehensive laws which guide the use and confidentiality of information systems.

Panel members stated that societal concern regarding an individual's right to privacy is balanced against the rights of the general public to access information stored by public agencies. They felt that the legislature will need to provide more guidance to agencies regarding when they must release information and when they must guard its privacy. It was generally agreed the development of these guidelines is inevitable and that they will make the imposition of court sanctions much less likely. They concluded that law enforcement would be best served by being proponents of workable policies, rather than the recipient of imposed restrictions.

Event-4 Terrorist destroys message switcher in Sacramento.

The panel used this event as an example of a multitude of potential problems. Regardless of the exact nature of the circumstances, it is inevitable that a major disruption will take place in the ability of California law enforcement to transmit messages between computers. A recent incident in New York City resulted in a total shutdown in Wall Street activity. This occurred despite a very modern system with built-in redundancy.

Event-5 Federal Government enacts a national driver license system.

Panel members advocated some form of national identification system to identify individuals. They felt that, lacking the ability to uniquely identify individuals, large data base systems will be much less effective. Law enforcement has no way of identifying individuals without processing fingerprints. As data bases grow, individuals with the same names become increasingly frequent.

CROSS-IMPACT ANALYSIS

The purpose of cross-impact analysis is to generate a listing of alternative developments depicting the "most likely" future. It permits the researcher to analyze the consequences of implementing alternative policies. A cross-impact analysis is a forecast based upon the assumption that each of the "events" actually takes place. The forecast is the impact that the event would have on each of the other events and the trends. This cross-impact analysis was conducted by a group of seven persons representing law enforcement management as well as computer systems management.[8]

In selecting events for further discussion, those events having the most potential impact on other events and trends were given priority.

Event-1. State Mandates a State-Wide System and Makes Funding Available (6 event impacts)

This event becomes the catalyst to make networked systems in California become a

[8] See Appendix B.

reality. The panel members felt that unless the system is both mandated and funded it has very little chance of becoming a reality. Further, panel members concluded that many of California's larger agencies will be reluctant or unwilling to work cooperatively to network these systems. Their fears were confirmed by both the literature search and interviews. Resistance to change is cited as a major obstacle to the type of cooperation considered necessary.

Event-2. Court Rules that Electronically Stored Information is not Admissible in Court. (6 event impacts)

This event had a strong negative impact upon the issue. Panelists felt that severe court restrictions would render systems virtually useless. This event would also negatively impact upon the trends critical to this issue. However, they also felt that the chance for this event happening was very low. In fact, the panel median rated the event a zero per-cent chance of taking place. They assumed that the state would work to pass laws which limit the possibility for abuse and an adverse court ruling. They also stated that all of society has become reliant on networked systems, including the courts.

Event-5. Federal Government Enacts National Driver License System (6 event impacts)

This event was designed by the NGT group to provide a positive means of identifying an individual person. The ability to positively identify an individual through the use

of a unique number was believed to have a strongly favorable impact on the individual concern for the right to privacy and the standardization of data collection, storage and use. The standardization issue was cited as a major obstacle to systems networking by nearly every expert consulted during this research. This problem has been compounded by the influx of immigrants into the state. First and last names are used interchangeably in some regions of the world. This leads to great uncertainty regarding how the name should be stored or retrieved and makes the task of positive identification much more difficult.

Table 1 Basic Cross-Impact Evaluation Matrix

IMPACTING EVENT (Actors)	IMPACTED EVENT (Actors)					IMPACTED TRENDS (Reactors)					Impact
	E1	E2	E3	E4	E5	T1	T2	T3	T4	T5	Event Impacts
E1 State mandates a state-wide system and makes funding available.		_	-75	+50	_	+70	+100	+100	_	+100	6
E2 Court rules that electronically stored information is not admissible in court.	-75		+40	_	_	-10	-20	-80	_	-10	6
E3 Legislature passes comprehensive laws which restrict the use and security of information systems.	-50	-50		_	_	-10	-20	_	_	_	4
E4 Terrorist destroys message switcher in Sacramento.	+25	_	_		+10	+10	_	_	_	+10	4
E5 Federal Government enacts a national driver license system.	+90	+10	_	_		+10	+200	+200	_	+30	6
EVENT AND TREND REACTORS (Impacts or "Hits")	4	2	2	1	1	5	4	3	0	4	

Legend

T1 Funding for computerization.

T2 Individual concern regarding right to privacy.

T3 Standardized methods for the collection and retention of information.

T4 Public expectation of police role as "service providers."

T5 The rate of change of technology.

NOTE: The table shows the impact of events if they were to happen. This is measured against each of the other events and the trends. The impact is measured by the percentage of increase or decrease to the forecast level. N = 7 (All measurements are the maximum impact the event would have on other events and trends. The impact is shown as a "+" or "-" percentage.)

FUTURES SCENARIOS

A scenario is a narrative which sounds as if it were written by a historian looking back over the trends and events of a given time frame. It shows the reader what could happen if various combinations of trends and events occurred as forecast.

The data which was discussed earlier lacks a framework against which a reader might develop a vision of the future. The data discusses bits and pieces without presenting a whole picture. The following scenarios are presented to depict alternative images of the future. Each was constructed based upon data generated by the group forecasting process, the literature search and interviews.

Exploratory: "Surprise Free" [9]

"TECHNOLOGY ADVANCES WHILE LAW ENFORCEMENT STAGNATES"

Computerworld, February 23, 2001

"GOVERNOR JERRY BROWN INHERITS $25 BILLION BUDGET DEFICIT" Sacramento Bee, January 15, 2001

Bill shifted nervously in his chair as he waited for Sergeant Edwards to begin his three-month performance appraisal. He wasn't sure how the evaluation would turn out, but he knew that he'd done his best to learn the job of Records Clerk. "Police work is sure a lot different than I'd

---

[9] This scenario is based on an assumption that the forecast events did not happen. No cross-impact data is incorporated because none of the events happened. It incorporates issue-related events which have been occurring in the past. The medians of the ""will be" forecasts are incorporated. Trends are included where the writer has confidence in the forecasts. This scenario allows the present set of trends to "play out" into the future with today's attitudes, standards and policies. In other words, it tells the reader what might happen - if nothing is done to change the future course.

imagined," he thought. Bill thought back to his days with Federal Express as a shipping clerk and contrasted his experiences there with his new job for the Sheriff's Department.

His daydreaming was suddenly interrupted as Edwards cleared his throat and began to speak. "Looks like things have gone pretty well for you. The other Records people seem to like you and your work meets our standards. We were lucky to get you - most of our new employees don't have much on the ball - our salary range doesn't match private industry. Why in the world did you leave FedEx to work for us?" This was the one question Bill dreaded discussing. He had to talk to the Background Investigator about it, and now this guy wanted to bring the subject up all over again. Bill nervously began to tell the story again. "Well, it was for theft. You know, it wasn't much. Just an undeliverable package. They have a rule against taking anything. I guess they considered it stealing. It really wasn't worth much..."

Suddenly Sergeant Edwards cut him off, "Hey, that's okay. Our department has different standards - we try to rehabilitate people. Don't let it get you down. With the cutbacks in state funding we can't afford to hire people with really clean records. Like I told you, we feel really lucky to get you!. Now, tell me what you think of our records operation."

Bill felt better, the focus was off of him and back on the job. "Actually, it's really pretty old technology. I mean, I'm just not used to all the typing. We get a hand written report from the officers, we type it into our computer system, then we have to re-enter the information into the regional and state systems. Seems like a lot of redundant work to me."

Edwards suddenly cut him off, "You should feel lucky. We just recently purchased that computer system. Most departments are still using something called alpha cards and maintain their records systems by hand. If it wasn't for asset seizure money we'd still be doing it the same way.

Sure, we lose information once in awhile. Just last week we let a rape suspect go without charges 'cause we didn't know that the Detectives were looking for him. Look, we've spent more than enough time on this interview. I've got a ton of work to do and we should both get on with it. Keep up the good work and you'll get along just fine."

As Bill walked back to the Records Section he thought, "Well, this place may not be run as well as FedEx, but I guess I'm pretty lucky to have a job at all."

Hypothetical: "What-If" [10]

"CALIFORNIA BECOMES FIRST STATE IN UNION TO LINK ALL POLICE DATABASES" Police Technology News, March 2001

"NATIONAL IDENTITY CARD BLASTED BY ACLU" San Francisco Chronicle, July 18, 1997

"LEGISLATION TO LIMIT COP'S COMPUTERS DEFEATED" California Legal Reporter. April 1998

They stood around the body, watching the ID Tech methodically doing the detailed work of searching for clues. The search for hairs, fibers, latent prints, and DNA samples continued. Lieutenant Nguyen, growing impatient, asked the ID Tech, "how much longer is this going to take, we've been here fifteen minutes already! If you don't get your butt in gear the guy who did this

---

[10] This hypothetical mode scenario is a demonstration of a possible, but improbable future. It is assumed that certain events will happen and describes the future. All of the forecast events having a positive or "good" impact on the issue have been allowed to happen. Additionally, materials from the literature search which reflect positive impact on the issue are included. This is not a likely future because it is very unlikely that both the funding and the determination to make it happen will exist.

will be on the other side of the damn country."

"Sorry Lieutenant, but I'm having a little trouble with the latent fingerprint imaging system. It's probably the satellite communications downlink, they still have trouble with sunspot interference. You'd think that if they can put a man on Mars they could make one of these that could work all the time."

As she stood there impatiently, Nguyen saw the green light glow brightly as the machine indicated direct communication with the state's Police Criminal Information Network. This told her that the latent images were being scanned and fed by computer directly into the statewide message switching system. The digitized images, based on the old Cal-ID system were being searched against the databases of California's more than six hundred police agencies.

"Okay, looks like we got a hit," the ID Tech called out. They both watched the display screen as the results of the database search came back. The name of a suspect appeared on the screen showing a positive match of the latent just scanned against the state's criminal files. Their suspect had a long history of violent sex offenses and was well known to the criminal justice system. The machine came to life again as it displayed the results of a name search it had just completed.

The Lieutenant smiled broadly and said, "What do you know, Santa Clarita just booked this guy as a drunk driver twenty minutes ago. Probably picked him up right after he left here. Looks like we can close this case out before lunch. Good work, Trahn, let's get out of here."

Normative: "Desired and Attainable" [11]

"REGIONAL POLICE COMPUTERS LINKED TOGETHER" CPOA Journal, November 1997

"SANTA CLARITA CHIEF BLASTED- GUN POLICY QUESTIONED" Santa Clarita Times Tribune, March 18, 1999

"Look Chief, I don't know what the big hassle is. Jack never had any trouble issuing me my gun permit before. What's the big deal?"

Chief Roberts had heard this same story before. Since she had taken over the Santa Clarita Police Department, one of her biggest headaches had been to reduce the number of Concealed Weapon Permits issued by her predecessor. She looked over the file. The guy owned a pawn shop, carried large sums of cash in the course of his business and had no prior arrests. He had been mugged a few times and she really didn't see any reason to turn him down. Still, she had a funny feeling about this one.

"Thank you for your patience, just one more thing to do," she said as she entered his name into COPS. That's the acronym for the newly-installed Criminal Offender Profiling System. The department could never have afforded this technology, but legislation enacted by the state last year mandated such a system and provided the funding. Following a quick search of the state-wide alpha system, the machine made a quiet beeping sound indicating it had completed its task.

"Mr. Ryan, I know you've never been arrested before, but tell me about this incident in Los

---

[11] This scenario is a demonstration of a desired end-state in the future through a distinct and plausible path of events. It concentrates on "should be" data from the trend forecasts. Events from the cross-impact evaluation are included which are both positive events and which impact other events and trends. It also includes information from the literature search which is considered positive by the writer.

Angeles last week," she said.

"Hey, that was no big deal," he replied. "I had a few too many drinks in a bar. Some guy pushed me around and I had to protect myself. I pulled out my gun and he backed right off. The bartender called the cops. Thank God I've got a permit for this thing. What's the problem? The cop said everything was OK, that he'd just fill out something called an FI card."

"That's a Field Interview Card," she responded. "They entered it into the system and our database search picked it up." The Chief smiled inwardly and thought, "Looks like I'll be able to deny this renewal. I didn't like the looks of this guy anyway, seems like a real jerk." Chief Roberts turned to the applicant and said, "I'm awfully sorry Mr. Ryan. I will be unable to issue you a renewal. Our permits clearly state that you cannot frequent bars or consume alcoholic beverages while carrying a gun. But, you can reapply in a year and I'm sure we can work something out. By the way, tell the Mayor I said 'hello' the next time you see her."

As Ryan walked out of the Chief's Office she nearly muttered aloud what she was thinking, "What a jerk! Without COPS, that guy might still be out there wearing a gun with my permission."

Conclusion:

The futures study utilized personal interviews, a literature search and a group forecasting process to define the trends and events impacting upon the issue of networked law enforcement information systems in California. These trends and events were used as the basis for constructing possible future scenarios. Defining and understanding possible future scenarios permits law enforcement executives to create policies which will either assist in making a desired future occur, or prevent an undesireable future.

This study focuses on the sharing of automated information by California law enforcement agencies by the year 2000. This issue was further defined and limited by the sub-issues previously identified. These limits were made necessary by the availability of time and financial resources available to devote to the study.

SECTION TWO: STRATEGIC MANAGEMENT

A PLAN FOR MANAGING LAW ENFORCEMENT

INFORMATION SYSTEMS TECHNOLOGY

A PLAN FOR MANAGING LAW ENFORCEMENT INFORMATION SYSTEMS TECHNOLOGY

The normative mode scenario was selected as the basis for the development of a strategic plan.[12] This scenario depicts a future which is both desirable and attainable by California law enforcement. The following represent elements of the desired future developed from a review of the futures research and will provide a focus for this section:

- Police department record systems are linked electronically, permitting searches on a regional and state-wide basis.
- Exposure to civil liability caused by the misuse of information is minimized.
- Systems are developed in the most cost-effective way, with redundancy minimized.
- The market is driven by the needs of law enforcement, not the needs of the vendors.
- Agencies work together cooperatively to share information, rather than developing and protecting their individual feifdoms.
- The public accepts the sharing of information by law enforcement as necessary to public safety. They do not view it as another threat from "Big Brother."
- Computer systems receive sufficient funding to meet the needs of law enforcement.
- Police agencies do not misuse the information shared electronically, reducing the potential that courts will rule adversely against its use.

---

[12] The environment assessment, the mission statements and the situational analysis were developed with the cooperation of a three-member panel of law enforcement executives.

MISSION STATEMENT

Macro The mission of the state-wide law enforcement information system is to provide an automated means by which California law enforcement agencies are able to share criminal information which enhances their ability to prevent crime, apprehend and prosecute violators and return property to its rightful owners.

Micro Law enforcement agencies will be encouraged to form regional information systems designed to best serve the needs of their agencies and the public in that region. These regional systems will be encouraged to share information with one another by means of the state-wide system.

SITUATIONAL ANALYSIS

The situational analysis measures the effect of previously identified trends and events upon the organization.

Environmental Factors: Environmental factors can be viewed as opportunities and threats as they apply to the external environment of the organization. These are factors which are beyond the direct control of the agency. In this case, the "agency" consists of groups of law enforcement agencies which have joined together to share automated information. The following were developed by a small-group process designed to measure the readiness and capability of the organization to change.

Opportunities:

- Rapidly developing technology providing greater potential for networking systems.
- Strong public support for law enforcement programs.
- Alternative sources of funding for law enforcement programs.
- More reliable systems at lower cost.
- Cost-effectiveness of automated systems.

Threats:

- Rapidly changing technology means agencies will be at very different levels of sophistication, depending upon funding resources. This will hamper networking efforts.
- Public fear of computer databases.
- Susceptibility of system to hackers, terrorists, natural disasters and disgruntled employees.
- Restrictive court rulings or legislation which limits the effective use of information.
- Lack of funding.

Internal Assessment: The trends and events can also be viewed from the perspective of the agency itself and are described as weaknesses and strengths of the agency.

Strengths:

- Law enforcement officials and their agencies have strong ties with one another and have proven that they can work cooperatively to solve problems.
- All law enforcement agencies share a need to investigate crimes more effectively.

- The police profession has played a leadership role in adopting new technology.

Weaknesses:

- Information systems which address a very narrow range of needs and which do not share information with other systems. The State of California funds the development of systems which are intended to address one issue only, such as sexual assaults, serial homicide or gangs. These systems are generally independent of other systems and serve a narrow spectrum of law enforcement's needs. The concern with these systems is that they divert funding and attention from other projects which could serve a broader range of law enforcement needs.
- Many agencies prefer to develop their own report formats and reporting systems, making networking more difficult and more expensive.
- Agencies and regions with successful systems may fear changes designed to provide networking with other agencies or regions.

STRATEGIC ASSUMPTION SURFACING TECHNIQUE

Stakeholder Analysis: Stakeholders are individuals or groups who are: impacted by the organization, are able to impact the organization, or are concerned about the issue or the organization. The following groups and individuals were identified as meeting this criteria.

Stakeholders:

1. Sheriffs and Chiefs
2. Police Records Personnel
3. Patrol Officers
4. Taxpayer groups
5. Local elected officials
6. State elected officials
7. State Attorney General
8. Federal Bureau of Investigation
9. Commission on Peace Officer Standards and Training
10. Police management organizations
11. Police unions
12. Information System Vendors
13. News Media
14. Civil Liberties Groups
15. Prosecutors
16. Defense Attorneys
17. Criminal Investigators
18. State Attorney General
19. Information Systems Managers
20. Users of Existing Regional Inform Systems
21. Law enforcement support groups
22. Victim rights groups
23. Minority groups
24. The Court System

Stakeholder Assumptions:

Those stakeholders which were considered to be the most likely to significantly impact the issue and sub-issues were selected from this list for further analysis. The following assumptions were developed for these stakeholders.[13]

Sheriffs and Chiefs (SUPPORT)

1. Will resist changes to their present information systems.
2. Will expect someone else to pay for new information systems or changes to existing systems.
3. Will support systems which can assist them in accomplishing their agencies's missions.

Taxpayer groups (SUPPORT)

1. Will oppose any additional expenditure of funds supplied through direct or indirect taxation.
2. Will support changes which reduce numbers of paid personnel.
3. Will support proposals which make the most effective use of law enforcement resources.

Local Elected Officials (SUPPORT)

1. Will look to the state to pay for systems.
2. Will support programs which receive strong public support, are effective and are cost-effective.

State Elected Officials (SUPPORT)

1. Expect local jurisdictions to pay for what they receive.

---

[13] An assumption map was created with the assistance of a three-member panel. It can be found in Appendix B. It is useful in identifying the degree of certainty about these assumptions.

2. Will support systems which cross jurisdictional lines and serve the greater interests of the state as a whole.

3. Will support legislation protecting the rights of citizens to be free from government intrusion.

State agencies (SUPPORT)

1. Will accept a leadership role in networking systems if funding is provided.

2. Will resist changes resulting in diminished influence.

Police unions (NEUTRAL)

1. Will resist spending for information systems to the detriment of their interests such as salary, benefits and membership.

2. Will support systems which they see as legitimate crime-fighting tools.

Civil Liberties Groups (OPPOSE)

1. Will oppose any system which as perceived to threaten basic "rights."

2. Will look for problems to attack the credibility of the system.

3. Will encourage litigation designed to limit the usefulness of systems.

Regional Information System Users (SUPPORT)

1. Will oppose any changes which threaten their existing systems.

2. Will support efforts to link their regional systems.

POLICY ALTERNATIVES

The following alternatives were developed through a group process utilizing independent development and ranking of policies. The researcher modified the suggestions to avoid duplication and provide greater clarity.

Policy One: **Establish a State-Wide Technical Standards Committee**

Pros: Provides uniformity among agencies which will establish law enforcement as a more viable market for vendors.

Develops standardized communications interfaces which facilitate the access and searching of local and regional databases.

Establishes criteria for the positive identification of persons entered into the databases.

Establishes a system-wide security policy. This should include the use of a secure personal identification card based upon a biometric identification feature.

Cons: Some departments will reject or resist standards imposed by an outside agency.

Policy Two: **Law Enforcement Works to Establish State Laws Regulating the Security, and Release of Automated Information**

Pros: Reduces the possibility of other groups obtaining overly restrictive legislation.

Provides the basis for consistency between agencies. This will make it easier for courts, attorneys and the public to deal with various agencies.

Prohibits the use of any database information for any purpose other than criminal

investigations. Reduces the risk of adverse court rulings and diminishes the concerns of civil liberties groups.

Cons: Regulations will limit law enforcement prerogatives and could be so restrictive as to limit the effectiveness of the system.

Loss of local control.

Policy Three: Establish Locally-Controlled Regional Information Systems

Pros: Makes the most effective use of existing organizations and systems.

It is easier to gain consensus and support on a regional basis than on a state-wide basis.

Systems are more likely to address the needs of local law enforcement than systems designed and implemented by the state.

Cons: More difficult to ensure state-wide compatibility of systems.

Not as cost-effective as a single, state-wide system.

Policy Four: Mandate that Agencies Receiving State and Federal Funding Participate in Regional Information Systems, Adhere to Technical Standards and Agree to Share Information

Pros: Easier for regional information agencies to form.

Greater cooperation between agencies.

More cost-effective use of state and federal dollars by not duplicating systems which serve the needs of a single agency.

Cons: Some agencies will not support a system which will establish mandates.

Agencies may not accept state and federal funding with these restrictions.

Policy Five: **State to Establish a California Law Enforcement Technology Procurement Agency**

Pros: Standardizes equipment used within law enforcement information systems.

Makes quantity purchase and discounts possible.

Helps to make law enforcement a strong consumer in the computer market.

Reduces the time and cost of local research, development and procurement.

Cons: Limits the ability of computer vendors to control the market.

May subject the state to charges of unfair business practices.

Loss of local control if purchases through the agency are mandated.

RECOMMENDED STRATEGY

All five of the alternative policies would assist in making the desired future occur. Various strategies were considered for the implementation of these policies. Two strategies were considered by the panel. The criteria used for selection of the recommended strategy were: likelihood for support by the critical mass stakeholders, potential for success, cost-effectiveness, and the effectiveness of the completed system.

A series of regional information systems with common protocols for the sharing of information. This approach provides an optimum level of local control and will form the basis of local support. Previous attempts to establish large computer systems controlled by a central government agency have failed for a variety of agencies. One of the most frequently cited reasons is the failure to obtain a strong consensus and commitment of the participants. In a report presented

at a conference in 1990, Robert L. Marx of SEARCH Group Incorporated (a government funded computer research firm) stated, "Technological change occurs in the criminal justice community only when a broad consensus forms among the members of the community." [14] Many of the potential objections of key stakeholders were based upon the loss of local control to the state. By permitting and encouraging locally-controlled regional systems these objections are met.

Alternative Considered and Rejected: **A state-wide computer information system controlled by the State of California.** This strategy was rejected because it would take away local control from law enforcement agencies. This would establish a threat to existing systems and promote opposition by many Chiefs and Sheriffs throughout the state. In his report, Mr Marx also criticized the move of the late 60s to build "super systems." These were systems designed to meet the needs of law enforcement agencies, the court system, corrections, probation, parole, and others. He stated that, "it is a concept that required so much agreement from so many agencies who are unaccustomed to agreeing with each other that I think it fell from its own weight."

---

[14] U.S. Department of Justice, Office of Justice Programs, *Criminal Justice in the 1990's: The Future of Information Management,* (Sacramento, CA: SEARCH Group, Inc., April 1990)

IMPLEMENTATION PLAN

TIME LINE	ACTION STEPS
T	The Commission on California Peace Officer Standards and Training establishes an advisory committee to study the feasibility of a state-wide system of networked regional information systems.
T + 6 months	The Advisory Committee reports on the status of automated information sharing in California and makes a recommendation regarding the value and preliminary feasibility of a state-wide system.
T + 9 months	Assuming that the feasibility study establishes the need for such a system, POST prepares draft legislation which would address the needs of California law enforcement. The legislation would include the appointment of a Computer Task Force mandated to study this issue and report back its findings to the legislature.
T + 12 months	POST, working with Cal-Chiefs and Cal-State Sheriff's Associations find an author for the proposed legislation.
T + 18 months	Following passage of the proposed legislation, the State Legislature appoints Task Force members, including: Cal State Sheriffs, Cal-State Chiefs, the Governor's Office, and the California Department of Justice(Division of Law Enforcement).
T + 27 months	The Task Force conducts its feasibility study. During this process it builds support for the project by providing input into the process and educating potential benefits. It minimizes opposition by identifying objections and mitigating those which do not threaten the project. The feasibility study will address funding, participation in the system, access, rules for information use, standardization policies and needed legislation.
T + 30 months	The Task Force presents its report to the legislature with the support of the members.
T + 36 months	The State Legislature establishes a State-Wide Technical Standards Committee, provides funding for a "model" regional information system, provides funding for the development of technology necessary to permit the connection of regional systems through the use of the California Law Enforcement Teletype System (CLETS).
T + 42 months	The Technical Standards Committee develops mandates which must be met before agencies are eligible to receive state funding for computer systems.
T + 48 months	CLETS develops a plan to connect regional information systems.

TIME LINE	ACTION STEPS
T + 60 months	Two existing regional information systems establish a data link utilizing the protocols and access provided by the state through the CLETS system.

SECTION THREE: TRANSITION MANAGEMENT

MANAGING THE TRANSITION TO INTEGRATED REGIONAL INFORMATION SYSTEMS

MANAGING THE TRANSITION TO INTEGRATED REGIONAL INFORMATION SYSTEMS

Just as America's founding fathers rejected control imposed by the British, California law enforcement agencies have a strong tendency to reject authority imposed by state and federal agencies. Autonomy and the local control it implies are a driving force for the hundreds of law enforcement agencies in this state.

The proposal to network regional information systems maintains a high-degree of local control with the state taking an active role as a coordinating agency. This leaves local agencies able to make the vast majority of decisions impacting upon their own futures.

Selected Policies: The various policies and strategies formulated for the Strategic Plan were reviewed for consideration in the Transition Management Plan. Two criteria were used for inclusion. First, they had to be achievable. Second, they had to be something which law enforcement leaders could implement directly or through elected officials.

- **Establish a State-Wide Technical Standards Committee**
- **Law Enforcement Works to Establish State Laws Regulating the Security, and Release of Automated Information**
- **Establish Locally-Controlled Regional Information Systems**
- **Mandate that Agencies Receiving State and Federal Funding Participate in Regional Information Systems, Adhere to Technical Standards and Agree to Share Information**
- **State to Establish a California Law Enforcement Technology Procurement Agency**

Selected Strategy:

- **A series of regional information systems with common protocols for the sharing of information.**

MANAGEMENT STRUCTURE

The transition from the present-day situation to the desired future state will take considerable time and will require a different management structure. The Transition Management Team will be headed by a representative from the office of the California Attorney General, Division of Law Enforcement. The group will consist of representatives of the major constituencies, or "stakeholders," involved in the change. These include representatives from the Office of the Governor, the State Legislature, the California Police Chief's Association, and the California State Sheriff's Association. Their primary responsibility will be the oversight of the various state organizations and plans necessary to make this vision a reality.

In addition to the Transition Management Team described above, the following represents the minimum structure necessary to accomplish this change:

State-Level:

- **Technical Standards Committee** (Will develop the standards necessary to maximize the exchange of information between regional systems. These include networking protocols, length of data fields, and definition of terms.)
- **California Law Enforcement Teletype System** (Will provide the physical means of

transmitting information between participating regions through its message switching capability.)

- **California Law Enforcement Technology Procurement Agency** Supports the development of new technology for law enforcement. Acts as a purchasing agency for those agencies choosing to participate.

Regional Level:

- **Regional Information Systems** Regional systems have already been formed in some parts of the state. Joint powers agencies, chief's associations, and criminal justice agencies are organizations which can form the basis for the development of these systems. These agencies will perform a variety of functions, including: administration of the system, long-range planning, coordination with users, and coordination with the state.

Local Level:

- User agencies will form internal structures to coordinate internal computer system activities with those of the regional agency. These structures will include management, information system managers and system users.

COMMITMENT ANALYSIS

Critical Mass to Accomplish Change: The "Critical Mass" is the minimum number of people or groups necessary to implement the change. If any one of them is opposed to the change it will likely fail. However, it takes the support of all of them to succeed. It is assumed that the support

of some of these people or groups will deliver the support of others. For example, if the Police Chiefs support the change it is assumed that middle managers and information system managers will support the change. This should be true also for other groups such as police support groups and the general public.

Commitment Planning: The following illustrates the minimum level of support necessary from each member of the critical mass. If any of them fails to deliver the required level of support the project could fail. This also illustrates where the greatest effort will be needed. For example, little effort would be necessary for a person who is already committed to make the change happen. Conversely, anyone who will presently block the change requires more effort.

Table 2 Commitment Planning Chart

Key Players	Block Change	Let Change Happen	Help Change Happen	Make Change Happen
Chiefs and Sheriffs	X		O	
State Attorney General		X		O
State Elected Officials		X	O	
Local Elected Officials		X	O	
Regional Information System Users	X			O

Code: X = Where key players currently stand regarding this change.

O = Where key players will need to stand regarding this change.

Negotiating Acceptance: Negotiation with the members of the "critical mass" will be necessary to ensure the success of the plan. Since this plan involves law enforcement agencies throughout the State of California, no single set of strategies will be possible. The agencies range in size from one officer departments serving rural communities to some of the largest and most sophisticated agencies in the world.

For many years people have assumed that the only way to serve the state-wide information needs of law enforcement is to create a single computer system controlled by state government. One of the primary reasons for this plan was the inflexibility of hardware, software and operating systems. Networking of different types of computer systems was virtually unknown and early attempts were met with disaster.

In recent years private industry and the military have succeeded with advanced networking of previously incompatible systems. In the future, this networking capability will make today's attempts seem primitive by comparison. At a symposium on the future of law information systems held last year, one of the speakers from SEARCH Group Incorporated commented, "Ten years from now we won't care whether the data we handle are image or text, ten years from now we won't care how much data are needed, and ten years from now we won't care where data are located." [15] The persons interviewed for this project were in agreement with this statement.

What it means for law enforcement administrators of the future is that they will have few technological problems which they cannot overcome. This will leave people-oriented problems as the most difficult with which to deal. In fact, most of the information system administrators stated that these problems are already the most difficult. It is important that this distinction between "people problems" and "technical problems" be kept in mind when considering negotiations. For example, in the future the failure of an agency to adhere to technical standards will not be as difficult a problem as an agency's unwillingness to share information. One can be overcome by technicians while the other will require the cooperation of policy makers.

In reviewing the policies developed earlier, some were considered to be "negotiable." This means that failure to gain compliance will not doom the project to failure. Others, however, are considered to be so critical for success that they are "non-negotiable."

---

[15] *Principles and Predictions for Justice Information Management Systems*, Robert L. Marx, SEARCH Group (p. 25)

Negotiable:

Establish Locally-Controlled Regional Information Systems (While regional systems provide an effective means of serving the needs of law enforcement agencies, it is not the only model available which will permit the accomplishment of the primary purpose. Some agencies are so large that it may be impractical for them to participate in regional systems. However, they can still network with regional systems and share the information.)

State to Establish a California Law Enforcement Technology Procurement Agency (This procurement agency makes the acquisition of technology more cost-effective, but is not essential to this project.)

Establish a State-Wide Technical Standards Committee (Some technical standards are probably necessary, however the committee must use great care in not over-regulating this area. This could be counter-productive and actually hinder the efforts of some agencies to develop unique solutions to difficult problems.)

Non-Negotiable:

Establish Regulations for the Security, and Release of Automated Information (Some form of regulation already exists and should be expanded. This is critical because of the large volume of data to be stored, the number of people having access to the information and the potential for misuse. Failure to establish stringent guidelines with enforcement capability could expose the entire system to litigation or public scrutiny.)

Mandate that Agencies Receiving State and Federal Funding Participate in Regional Information Systems, Adhere to Technical Standards and Agree to Share Information (As

stated earlier, the only item in this group which is essential is the willingness to share information.)

SUPPORTING TECHNOLOGIES

Training Transition Managers: The California Commission on Peace Officer Standards and Training (POST) should work with the key stakeholders to develop training for top-level managers and mid-level managers. This training would be designed to educate these people about networking of computer systems and their advantages.

Conducting Professional Conferences: Few law enforcement administrators in California are aware of the availability of technology and the successes of various regional information systems. The State Attorney General should sponsor a conference to encourage agencies to work together to accomplish this goal.

Communication of the Vision: People at all levels of state and local government must join together to generate interest in this system.

- Professional articles need to be written and presented
- A professional group should be formed to explore the use of technology to solve information-sharing problems in California, identify solutions and generate interest in the idea
- The State of California, Cal Chiefs and Cal State Sheriffs should jointly author and adopt a blueprint for the future of law enforcement information systems networking. This plan would serve to guide agencies in their decision-making processes.

Responsibility Charting:

Responsibility charting was selected as a means of clarifying role relationships, as a means of reducing ambiguity, and as a means of ensuring that critical steps in the transition management process are completed. It identifies responsibilities for each of the key stakeholders identified earlier. It also identifies the responsibility of each person in completing key tasks during the transition and the specific role each is designated to perform.

Table 3 Responsibility Chart

DECISIONS	ACTORS						
	POST	State AG	State Chief's	State Sheriff's	Office of Governor	Office of Legislature	Regional System Rep
POST establishes an advisory committee.	R	S	S	S	I	I	I
POST prepares draft legislation.	R	S	S	S	S	S	I
Author found for legislation.	S	I	R	R	S	I	I
Legislation establishing Task Force passes, members appointed.	S	S	S	S	S	R	S
Task Force presents report to legislature.	S	S	S	S	S	S	S
Technical standards adopted.	S	R	S	S	S	S	S
CLETS develops networking plan.	I	R	S	S	S	S	S
Existing regional information systems linked.	I	I	S	S	S	S	R

Code: R = Responsibility (not necessarily authority)

A = Approval (right to veto)

S = Support (put resources toward)

I = Inform (to be consulted)

- = Irrelevant to this item

available dollars much more effectively. It would also provide a stronger reason for state and local policy-makers to provide additional funding needed for the system. By utilizing regional systems as the basis of a state-wide system, it permits the system to be developed incrementally as funds are made available.

AREAS FOR FURTHER STUDY

No study of information sharing can be all inclusive. The field is dynamic, literally changing from minute-to-minute. Many of the research materials gathered at the beginning of this project were found to be obsolete by the end of the project. The reader should note that the dates of most of the resource materials are less than six months old. This is a reflection of the constantly changing nature of the field. Included among the many areas worthy of further study are :

The Privatization of Information Systems: The public sector may not be the best providers of information systems to law enforcement. Given the number of agencies and incompatible systems in existence, one alternative worthy of examination is giving the job to the private sector. For example, San Diego County agencies reeling from the impacts of Proposition 13 (a property tax cutting measure enacted by California voters in the late 1970s) formed a publically-owned corporation to provide computer services. The San Diego Data Corporation now acts as a vendor for all types of services to county agencies. Though governed by a public board of directors, it acts much like a privately owned business. Since users may turn elsewhere for service, the corporation is obliged to provide the best service at

the lowest price.

The Commercialization of Law Enforcement Information: Those with a strong entrepreneurial spirit have advocated that local government do all it can to make money to support its programs. Should law enforcement provide access to names of burglary victims to alarm companies? A great deal of money could be made by policies such as this, but at what price? Would the public continue to hold law enforcement to same high level of esteem which it now enjoys?

The right of individuals to privacy versus the right of others to access government information.

A SEARCH Group study concluded that, "The private sector has become much more of a threat to personal autonomy and liberty than has the government at any level." [16] The writer cited examples such as medical testing, genetic screening, brain wave analysis, polygraphs, monitoring phone use, credit info, etc. However, the advancement of law information systems will mean that agencies will access vastly greater amounts of information about many more people. Some day, the public may well regard law enforcement with the same suspicions as the private sector.

Law enforcement has traditionally denied public access to its criminal files. However, the public and the press are demanding greater access. What will this mean to the

---

[16] *In the Beginning: A Review of Federal/State Information Law and Policies*, Carol G. Kaplan, Bureau of Justice Statistics, P. 47.

crime victim who does not want the information released? What will this mean to a police agency which no longer has absolute control over the information which it has gathered?

RECOMMENDATIONS Law enforcement has many options from which to choose for its information systems. This study has examined a few of those alternatives and advocated several changes. Clearly, the most important message is that a plan for the future is critical to make the best use of this valuable resource. The public would be appalled if it knew how little information sharing currently takes place. Now is the time to act before more valuable resources are misused on this fragmented and confusing system.

BIBLIOGRAPHY

Bay Area Governments, Association of (ABAG). Bay Vision 2000 (December 31, 1990).

California, Bureau of Criminal Identification. Status Report: California Identification (CAL-ID) System (January 1989).

California, Commission on POST. California Law Enforcement Training in the 1990's. A VISION OF EXCELLENCE (January 1991).

California, Commission on POST. Employment Data for California Law Enforcement 1988.

California, Economic Development Corporation. VISION: California 2010 (March 1988).

California, Department of Justice. A Survey to Determine the Need for New Data Bases in the DOJ CAL-INFO System (June 1990)

California, Department of Justice. Special Agent 2000, Moving Toward the Future (Jones, 1991).

California, Information Technology, Office of. How to Plan for Managing Information (October 1987).

California, Information Technology, Office of. Strategic Direction for Information Technology in State Government 1988-1993 (June 1988).

U.S. Office of Technology Assessment. Science Technology and the Constitution (September 1987).

U.S. Department of Justice, Office of Justice Programs. Criminal Justice in the 1990's: The Future of Information Management April 1990).

U.S. Department of Justice, Office of Justice Programs. Criminal Justice Information Policy: Original Records of Entry (November 1990).

U.S. Department of Justice, National Institute of Justice. The Criminal Justice Microcomputer Guide and Software Catalogue (June 1988).

U.S. Department of Justice, National Institute of Justice. Directory of Criminal Justice Information Sources (September 1989).

Wozniak, Chris Internetworking: An Introduction (Palo Alto: Wollongong Group, Inc. 1988).

KEY TERMS [17]

Database: Information stored in a computer for subsequent retrieval.

Dataprocessing: The process of converting data into information and the manipulation, storage and retrieval of that information.

Criminal Information: Information collected and retained by law enforcement agencies which relate to specific criminal acts or pre-criminal conduct of individuals or groups of individuals.

Hacker: A person who attempts or completes an unauthorized entry into a computer system by electronic means.

Hardware: The physical equipment of a computer system consisting of electrical and mechanical components.

Network: A system of interconnected computers which send and receive data and messages via cable or some other communications medium. (See Appendix C for system illustrations)

- **Centralized Network:** All data is stored on one large computer with users sending information to and receiving information from the database.

---

[17] U.S. Department of Justice, National Institute of Justice. The Criminal Justice Microcomputer Guide and Software Catalogue (June 1988). Most of the following definitions were taken from this source. Others are from various professional publications or consultants.

- **Hierarchical Network:** Data is stored at regional and centralized databases. Queries to the system are first made against the regional database, then against the centralized database.

- **Decentralized Networks:** Information is stored in local, regional and central databases. Queries may be made directly to any of these storage facilities.

Information: Criminal history data, modus operandi, reports of crimes, photographs, fingerprints, intelligence reports,

Nominal Group Technique: The Nominal Group Technique (NGT) is a small group technique for achieving agreement on the answer to a single, usually complex, question by a process that alternates private work and open discussion.

Protocol: A set of procedures or conventions used routinely for determining how and when to format and send data between computers.

System: All of the equipment, personnel, material, procedures, documentation and information which forms a self-sufficient unit capable of attaining specified objectives.

Transmission: The process of sending information by computer networks, radio, telephone, FAX, writing, or satellite.

Appendix B - Futures Study

(NOTE: The following letter was sent to Nominal Group Technique panel members to prepare them for the process. The members were all knowledgeable about local government and information systems technology. The Nominal Group Technique (NGT) is a small group technique for achieving agreement on the answer to a single, usually complex, question by a process that alternates private work and open discussion.)

DATE: *Thursday, January 24, 1991*

TIME: *9:00am to 3:00pm*

LOCATION: *Piedmont Police Department, Memorial Room*
403 Highland Avenue

ISSUE

Issue: "What problems will California law enforcement agencies face when sharing criminal investigation information by the year 2000?"

Sub-Issue: Police agency resistance to changing their information systems.

Sub-Issue: Ability of police agencies to fund information systems.

Appendix B - Futures Study

In order to give you a better idea about where I'm headed on this issue, the following is the introduction from my project proposal:

> The time is 3:30pm, February 18, 2000.
>
> *An investigator in Redding is working on a particularly brutal series of rapes and runs his list of suspects through COPS (the California Criminal Offender Profile System). He learns that one of them was a suspect in a similar case in Sacramento last week. The information gained from Sacramento leads to a successful prosecution.*
>
> This scenario could not happen today. Most databases maintained by California Law Enforcement agencies are not networked. Instead, information exchange depends upon old-fashioned means, such as word-of-mouth.
>
> However, agencies in several parts of the state are working to change this. Departments in San Diego County, Orange County and Santa Cruz County have already developed regional systems with networked computers, while Alameda County and Contra Costa County have systems which are under development.
>
> The growth of networked systems will assist law enforcement agencies, particularly in the area of criminal investigations. Along with these rewards, agency administrators will have to face many challenges when managing this new technology.
>
> This research project will: provide background data on the issue and its importance, define the scope of the study, identify the problems which will be faced by tomorrow's chief executives and propose solutions to deal with them.

We will be using the Nominal Group Technique (NGT) to develop a forecast of the future as it relates to this issue. Each of the nine members of the discussion group bring a special area of expertise about networking computer systems.

Phase 1: **TRENDS**

a. Using the attached list as a starting point, develop a list of trends which impact upon the issue and sub-issues. (i.e. Level of computer literacy among employees.)

a. Identify the 7-9 trends, in rank order, which are most likely to have an impact on the issue and sub-issues.

b. For purposes of top-level strategic planning, how important would it be to have a long-range forecast of the trend? The list will be narrowed to those which would be most valuable.

Phase 2: **EVENTS**

a. Using the attached list as a starting point, develop a list of events which impact upon the issue and sub-issues. (i.e. California mandates standards for data-

interchange.)

b. Identify the 7-9 events, in rank order, which would probably have an impact on the issue and sub-issues, if they were to occur.

c. Only retain events which can be affected by prior policy. Do not include natural disasters or other events over which we have no influence or control.

Phase 3: **FORECASTING**

a. Each person will forecast what the trend level **will be** in 5 years and ten years and also **what it should be.**

b. Each person will then forecast when each event could occur and its probability of happening.

Phase 4: **CROSS-IMPACT EVALUATION**

a. Each group member will be asked to forecast the impact that would occur if an event actually happened. The impact will be forecast for each other event and against each of the trends.

Phase 5: **DISCUSSION OF THE FUTURE** The most productive part of the day should be this discussion. Based upon the foundation which we have prepared we need to develop a scenario of what the future should look like. What policies are necessary to help this most desired future take place? What do we need to do to make sure that negative events do not take place?

Appendix B - Futures Study

TRENDS

Social:

Ability of defense attorneys to access information through discovery.

Admissibility of computerized information as evidence.

Computer literacy of police employees.

Accuracy of information in police files.

Legislation or judicial rulings which limit information sharing.

Individual concern regarding right to privacy.

Number of crimes.

Right of named individuals to access files.

Volume of information collected by law enforcement.

Mobility of population.

Growth of metropolitan areas.

Willingness of agencies and investigators to share information.

Standardized methods for the collection and retention of information.

Level of information sharing.

Public fear of computerized databases.

Susceptibility of police employees to bribes.

Technical:

State of technology.

Transmission means.

Appendix B - Futures Study

Hardware and software compatibility.

Ability of systems to be interconnected.

Ease with which systems can be used.

Reliability of systems.

Economic:

Competition with high-profile systems. (VICAP, Serial murders)

Cost of information sharing.

Funding for law enforcement services.

Funding for computerization.

Cost-effectiveness of shared information in solving crimes.

Competition with other governmental agencies for funding.

Political:

Legally mandated information sharing.

Political sensitivity to "Big Brother" image.

Number of networked systems.

Willingness to fund systems.

EVENTS

Court rules that electronically stored information is not admissible in court.

ACLU wins large civil judgement following false arrest based upon information shared between police agencies.

A major police system is penetrated by a hacker and intelligence files changed.

Appendix B - Futures Study

Voice-activated information systems are placed into use by a major police department.

A records clerk accepts a bribe from a drug-dealer and erases intelligence information.

Courts severely restrict the sharing of information between law enforcement agencies, rendering automated systems virtually useless.

State mandates a state-wide system and makes funding available.

FBI mandates real-time reporting of crime information by law enforcement agencies.

Federal government mandates that all persons in this country be registered with law enforcement and be given a unique identification.

Legislature passes comprehensive laws which restrict the use and security of information systems.

Appendix B Futures Study

NGT PARTICIPANTS

Chief Joseph L. Colletti
Emeryville Police Department

Chief Pete Herley
Tiburon Police Department

Mr. Milt Kegley
Councilmember, Piedmont

Mr. Don Hubbard
President, DATA911

Detective Wally Briefs
Sunnyvale DPS

Lt. Bert Wilkinson, PIN Manager
Alameda County Sheriff's Department

Leila Dabscha
Records Supervisor, Pleasanton Police Department

Appendix B - Futures Study

Trends (as identified by the NGT group):

1. Ability of defense attorneys to access information through discovery.
2. Admissibility of computerized information as evidence.
3. Computer literacy of police employees.
4. Accuracy of information in police files.
5. Legislation or judicial rulings which limit information sharing.
6. Individual concern regarding right to privacy.
7. Number of crimes.
8. Right of named individuals to access files.
9. Volume of information collected by law enforcement.
10. Mobility of population.
11. Growth of metropolitan areas.
12. Willingness of agencies and investigators to share information.
13. Standardized methods for the collection and retention of information.
14. Level of information sharing.
15. Public fear of computerized databases.
16. Susceptibility of police employees to bribes.
17. State of technology.
18. Transmission means.
19. Hardware and software compatibility.
20. Ability of systems to be interconnected.

21. Ease with which systems can be used.

22. Reliability of systems.

23. Competition with high-profile systems. (VICAP, Serial murders)

24. Cost of information sharing.

25. Funding for law enforcement services.

26. Funding for computerization.

27. Value of shared information in solving recidivistic crimes. (are the systems worth what they cost?)

28. Competition with other governmental agencies for funding.

29. Legally mandated information sharing.

30. Political sensitivity to "Big Brother" image.

31. Number of networked systems.

32. Willingness to fund systems.

33. Dehumanization of system through technology.

34. Degree of access to information by public.

35. Level of restricted access to information by public.

36. Public expectation of police role as "service providers."

37. Nature of reported crimes.

38. Ability of government to fund information systems.

39. Vendor acceptance of standardization.

40. User demand for standards.

Appendix B - Futures Study

41. Stability of governmental agencies.
42. Degree of control over information access.
43. Degree of standardization of information collection.
44. The ability of agencies to pay for technology.
45. Degree of access permitted by individuals.
46. Public demand for accuracy of information.
47. The rate of change of technology.
48. Use of ergonomics to design information systems.
49. Qualifications for entry-level personnel.
50. Privatization of information systems.
51. Degree of local control over information contained in systems.
52. Number of "turn-key" information systems in use.
53. Impact of arrests on the criminal justice system.
54. The complexity of explaining information systems in a courtroom setting.
55. Degree of selling information contained in law enforcement information systems.
56. The ability of agencies to retain computer literate employees.
57. The ability of agencies to recruit computer literate employees.
58. The degree of pressure placed on law enforcement by the public to solve crimes.
59. The growth of networked "biometric" systems.

Appendix B - Futures Study

Events (as identified by the NGT group):

1. Court rules that electronically stored information is not admissible in court.

2. ACLU wins large civil judgement following false arrest based upon information shared between police agencies.

3. A major police system is penetrated by a hacker and intelligence files changed.

4. Voice-activated information systems are placed into use by a major police department.

5. A records clerk accepts a bribe from a drug-dealer and erases intelligence information.

6. Courts severely restrict the sharing of information between law enforcement agencies, rendering automated systems virtually useless.

7. State mandates a state-wide system and makes funding available.

8. FBI mandates real-time reporting of crime information by law enforcement agencies.

9. Federal government mandates that all persons in this country be registered with law enforcement and be given a unique identification.

10. Legislature passes comprehensive laws which restrict the use and security of information systems.

11. Proposition 13 overturned, court rules that property taxes must all be reduced to lower levels.

12. Sales tax revenues fall by 25%.

13. A disaster disrupts a major police information system for an extended period of time.

14. Terrorist destroys message switcher in Sacramento.

Appendix B - Futures Study

15. Gann initiative overturned.

16. Cal-Photo bill signed by Governor.

17. Law enforcement starts charging the public for access to police information systems as a means to raise revenue.

18. State-wide election changes focus of State government.

19. A world-wide currency is adopted.

20. Court rules that asset-forfeiture funds must go to General Fund.

21. Federal Government enacts a national driver license system.

22. Law enforcement official sells criminal information and causes major public outcry.

23. Major disaster diverts funds from law enforcement.

24. Private automobiles banned from urban freeway systems.

25. Legislature decriminalizes drug usage.

26. The Tokyo stock market collapses, recall of loans causes economic chaos.

27. High-profile media event results in restrictions on the use of criminal information.

28. A criminal suspect flees into outer space.

29. Information system compatibility is legislated.

30. Law enforcement is given access to Social Security Account Number information.

Appendix B - Futures Study

TREND GRAPHS

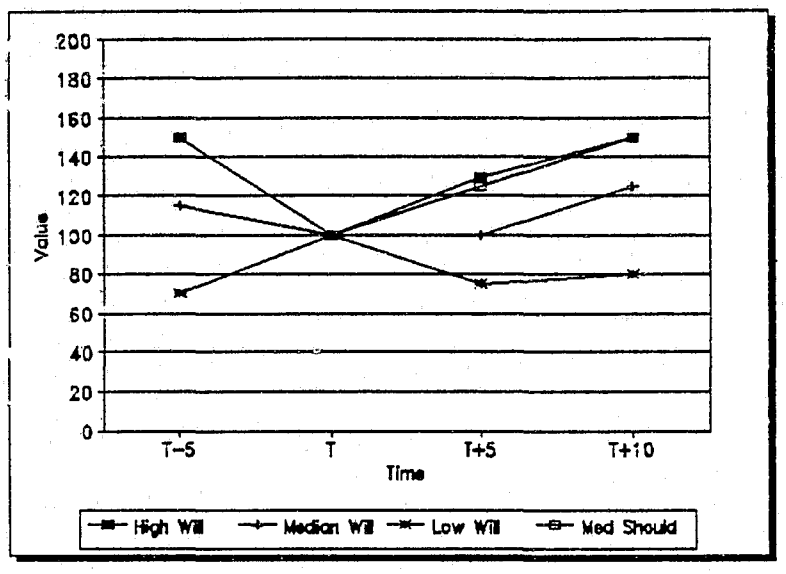


Table 4 Trend 1: Funding for Computerization

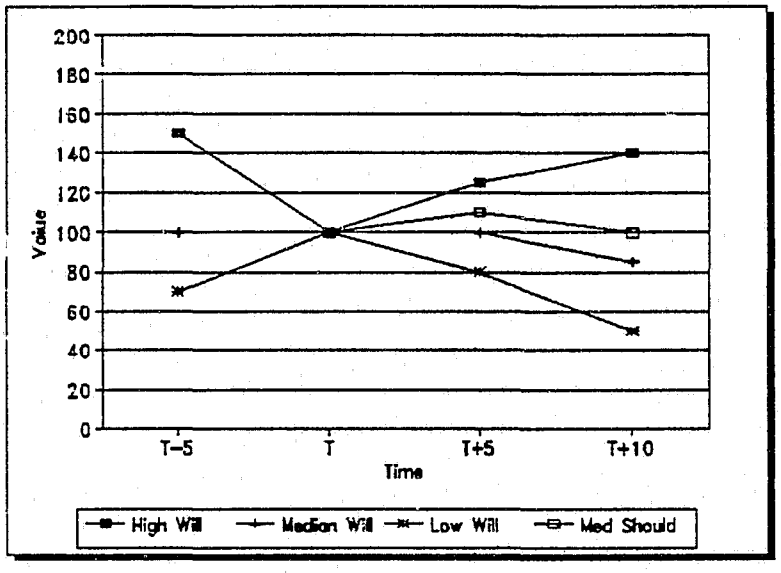


Table 5 Trend 2: Individual Concern Regarding Privacy

(NOTE: The Trend Graphs show panel medians for the high, median and low panel forecasts of what the trend was five years ago, and what it will be five and ten years from now. It also shows what the panel median of what the trend should be five and ten years from now.)

TREND GRAPHS

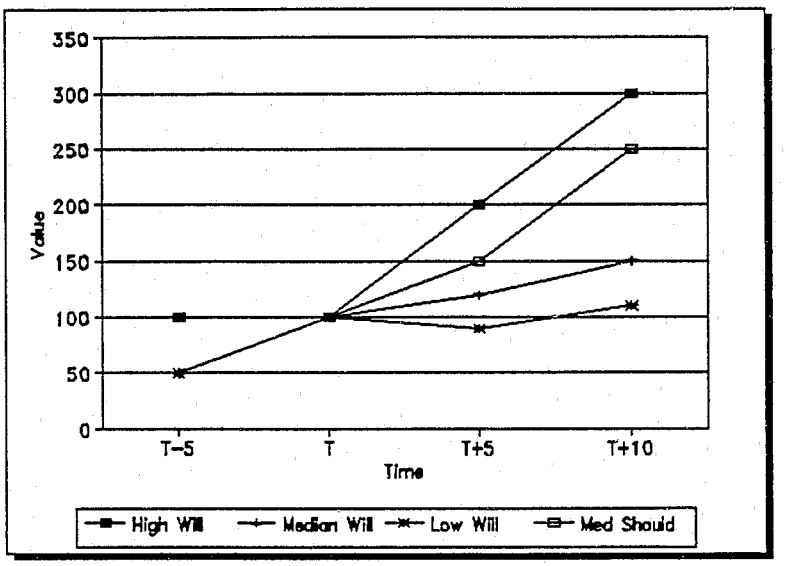


Table 6 Trend 3: Standardized Information Systems

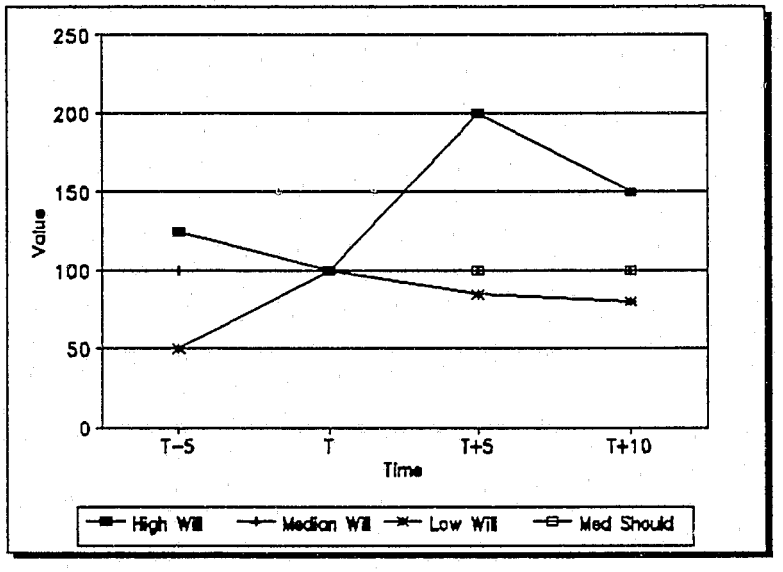


Table 7 Trend 4: Police Role as "Service Providers."

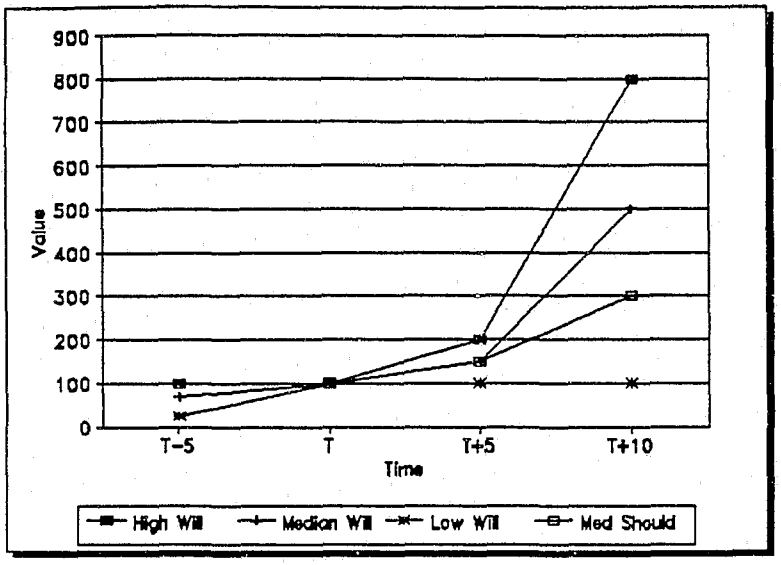


Table 8 Trend 5: Rate of Technology Change

EVENT GRAPHS

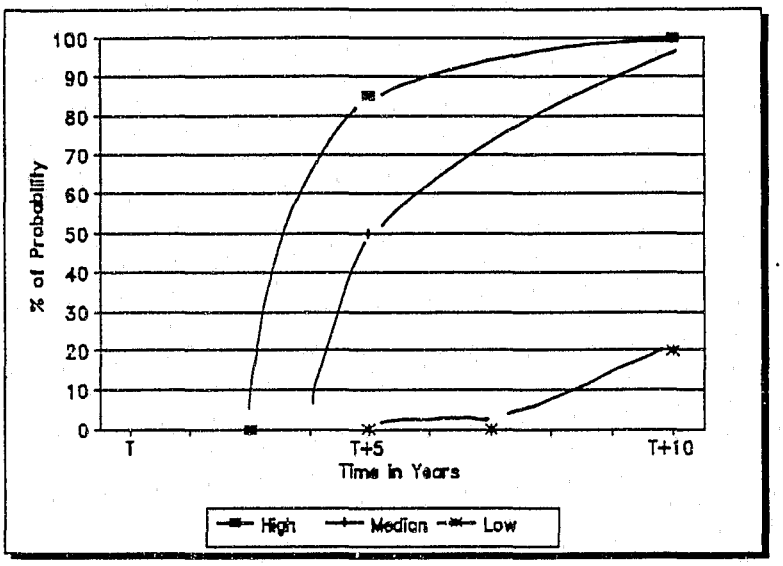


Table 9 Event 1: State Mandated Information Systems

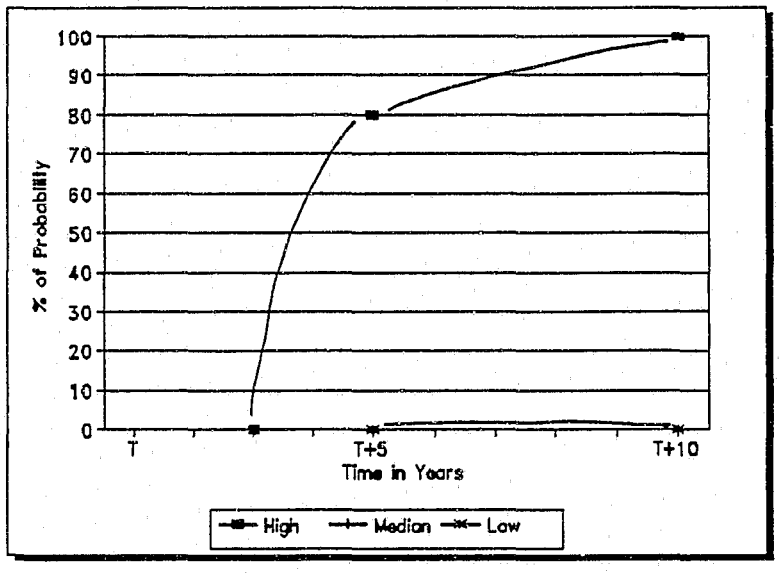


Table 10 Event 2: Court Rules Against Electronic Information

(NOTE: The Event Graphs show panel medians for the high, median and low forecasts. The mark on the 0% probability line displays the time in years when the probability that the event will take place exceeds 0%. A mark on the 100% probability line indicates that the panel median was that the event will definitely take place by the year shown.)

EVENT GRAPHS

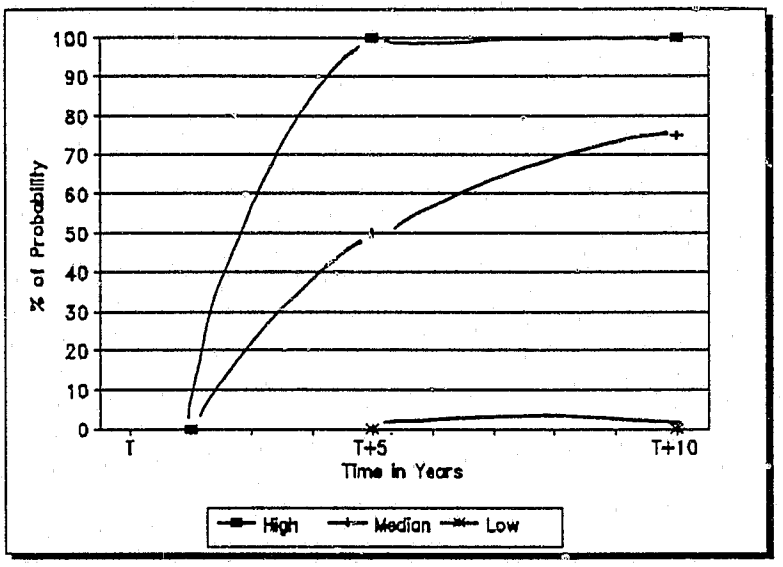


Table 11 Event 3: New Laws Restrict Use of Electronic Information

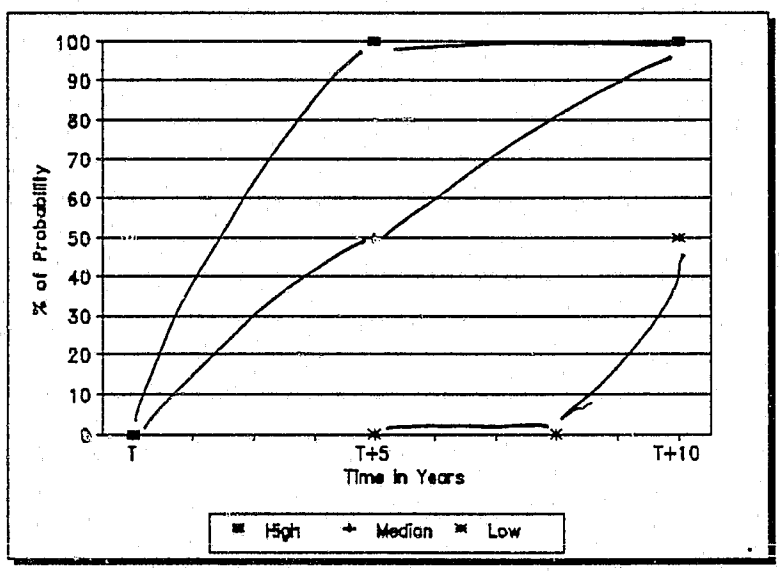


Table 12 Event 4: Terrorist Disrupts Network

EVENT GRAPHS

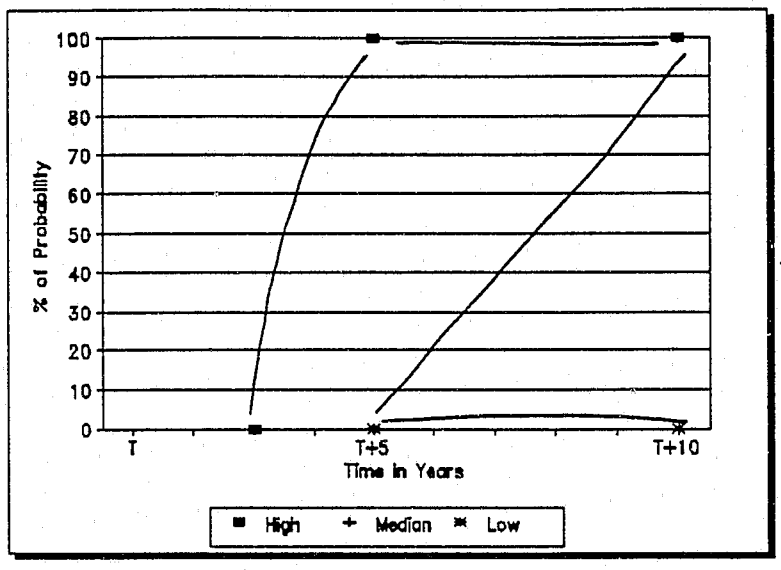


Table 13 Event 5: National Driver License

Table 14 Trend Evaluation Table

Trend #	TREND STATEMENT (Abbreviated)	LEVEL OF THE TREND** (Today = 100) 5 Years Ago	Today	* Five Years From Now	* Ten Years From Now
1	Funding for computerization.	115	100	100 / 125	125 / 150
2	Individual concern regarding right to privacy.	100	100	100 / 110	85 / 100
3	Standardized methods for the collection and retention of information.	50	100	120 / 150	150 / 250
4	Public expectation of police role as "service providers."	100	100	100 / 100	100 / 100
5	The rate of change of technology.	70	100	150 / 150	500 / 300

N = 7

** All number shown are median results of the panel.

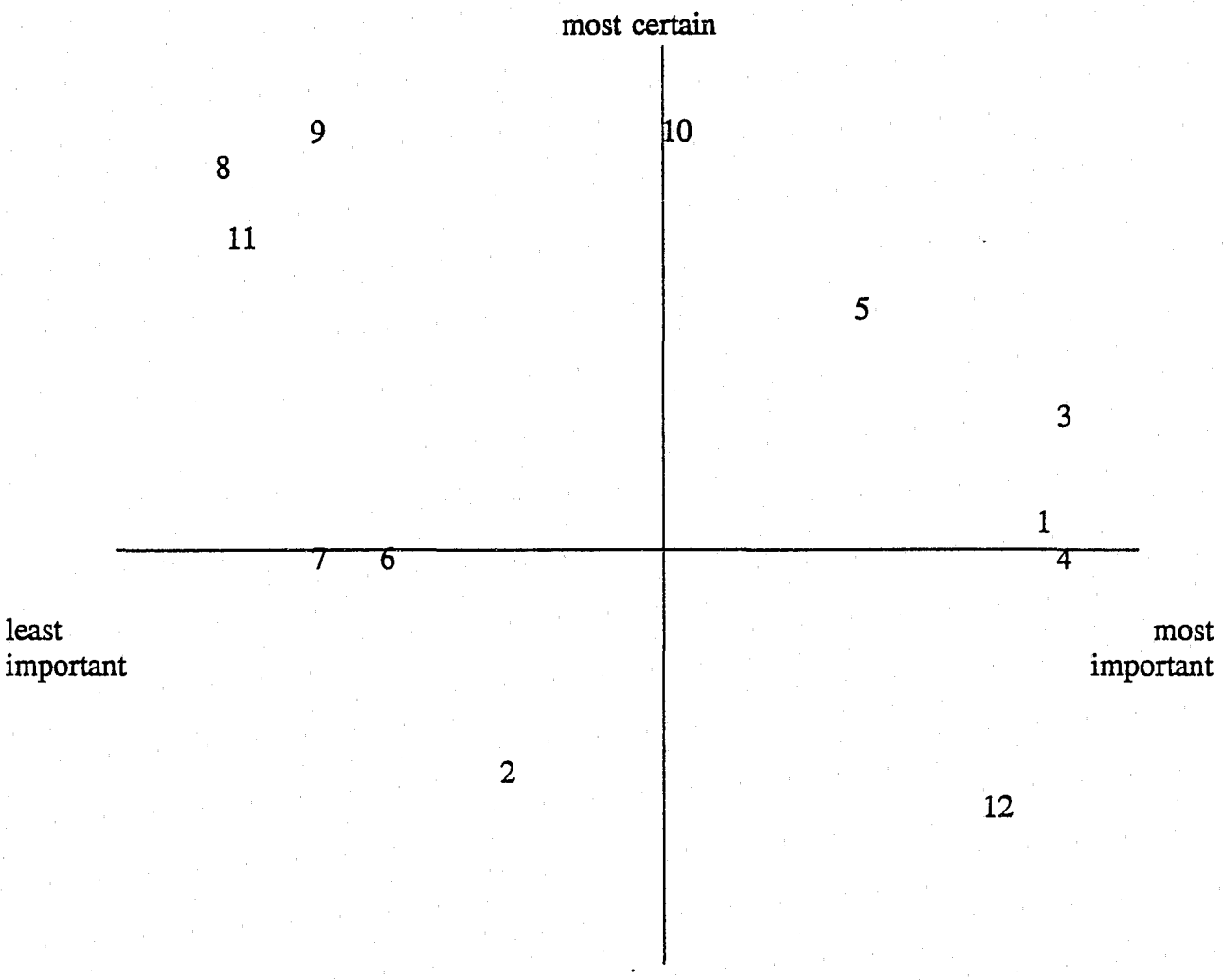
* "Will Be / Should Be" -

Table 15 Event Evaluation

#	CANDIDATE STATEMENT	Years Until Probability First Exceeds Zero	Probability that the event will take place. Five years from now (0-100%)	Ten years from now (0-100%)	Impact on the issue area if the event occurred Positive (0-10) scale	Negative (0-10) scale
1	State mandates a state-wide system and makes funding available.	5	50%	100%	10	0
2	Court rules that electronically stored information is not admissible in court.		0%	0%	0	8
3	Legislature passes comprehensive laws which restrict the use and security of information systems.	5	50%	75%	0	9
4	Terrorist destroys message switcher in Sacramento.	5	50%	100%	0	5
5	Federal Government enacts a national driver license system.	9	0%	100%	8	0

N = 7 All numbers shown are median results of the panel.

Figure 2 Assumption Mapping



1. Sheriffs and Chiefs
2. Taxpayer Groups
3. Local Elected Officials
4. State Elected Officials
5. State Agencies
6. Federal Agencies
7. Police Unions
8. Information System Vendors
9. Civil Liberties Groups
10. Prosecutors
11. Defense Attorneys
12. Regional Information System Users

Appendix C Strategic Management

(NOTE:The following letter was sent to Modified Policy Delphi Group members to prepare them for the process.)

DATE: June 25, 1991

TO: MODIFIED POLICY DELPHI GROUP

FROM: Tom Simms

SUBJ: **POLICY FORMULATION FOR COMMAND COLLEGE PROJECT**

The futures research for my Command College Project, "The Sharing of Criminal Investigation Information Among California Law Enforcement Agencies by the Year 2000" is complete. As part of that process various scenarios depicting the future of information sharing were developed. I have selected a Normative Mode scenario which represents a "Desired and Attainable" future.

The way to attain this desired future during the next ten years is to implement strategies and policies which will work towards that future. Each of you represents a different segment of this field, including: police administration, product development, consulting, records management, state government and regional information systems.

1. Proposed Policies: Please examine the following scenario from your personal and professional perspective. I would like each of you to then develop two or three policies or strategies to deal with this future environment. The strategy can be somewhat detailed, but should not exceed one paragraph. You do not need to type your response - just make sure its legible! Once completed, please fax your response to me. My fax number is **420-3002**. I would appreciate your response by Friday, April 26.

The policy or strategies can address the local, regional or statewide needs in this area. They should be policies or strategies over which law enforcement officials have control or significant influence.

2. Policy Ratings: After I review your proposed policies and strategies I will reduce the total number to approximately 8-10. There may be some editing where necessary. I will then fax the results to you and ask you to use the attached rating form. I will ask you to return the rating forms to me by fax ASAP.

3. Finalized Policies: Once I receive the ratings I will develop policies for use in the final paper.

ELEMENTS OF THE DESIRED FUTURE

- Police department record systems are linked electronically, permitting searches on a regional and state-wide basis.

- Exposure to civil liability caused by the misuse of information is minimized.

- Systems are developed in the most cost-effective way, with redundancy minimized.

- The market is driven by the needs of law enforcement, not the needs of the vendors.

- Agencies work together cooperatively to share information, rather than developing and protecting their individual feifdoms.

- The public accepts the sharing of information by law enforcement as necessary to public safety. They do not view it as another threat from "Big Brother."

- Computer systems receive sufficient funding to meet the needs of law enforcement.

- Police agencies do not misuse the information shared electronically, reducing the potential that courts will rule adversely against its use.

MODIFIED POLICY DELPHI GROUP

Chief Pete Herley
Tiburon Police Department

Detective Wally Briefs
Sunnyvale DPS

Leila Dabscha, Records Supervisor
Pleasanton Police Department

Robert B. Barnes
Consultant

Chuck Jones, Investigator
Department of Justice

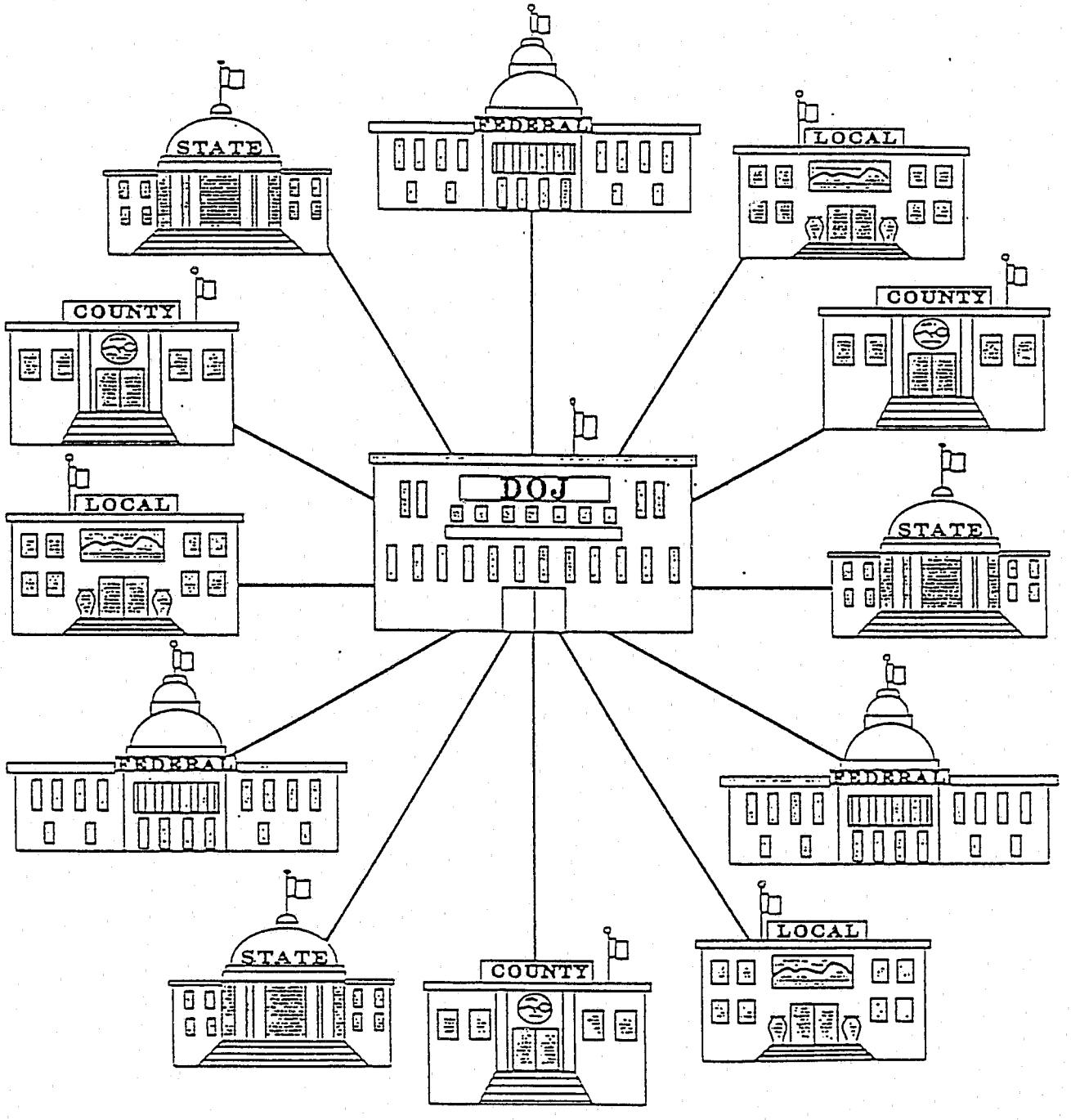
Bud Frank, Executive Director
Criminal Justice Council of Santa Cruz County

Nancy Angus, ARJIS Administrator
San Diego Data Processing Corporation

Captain Keith Jackson
Fremont Police Department

Lieutenant Ken Peterson
Milpitas Police Department

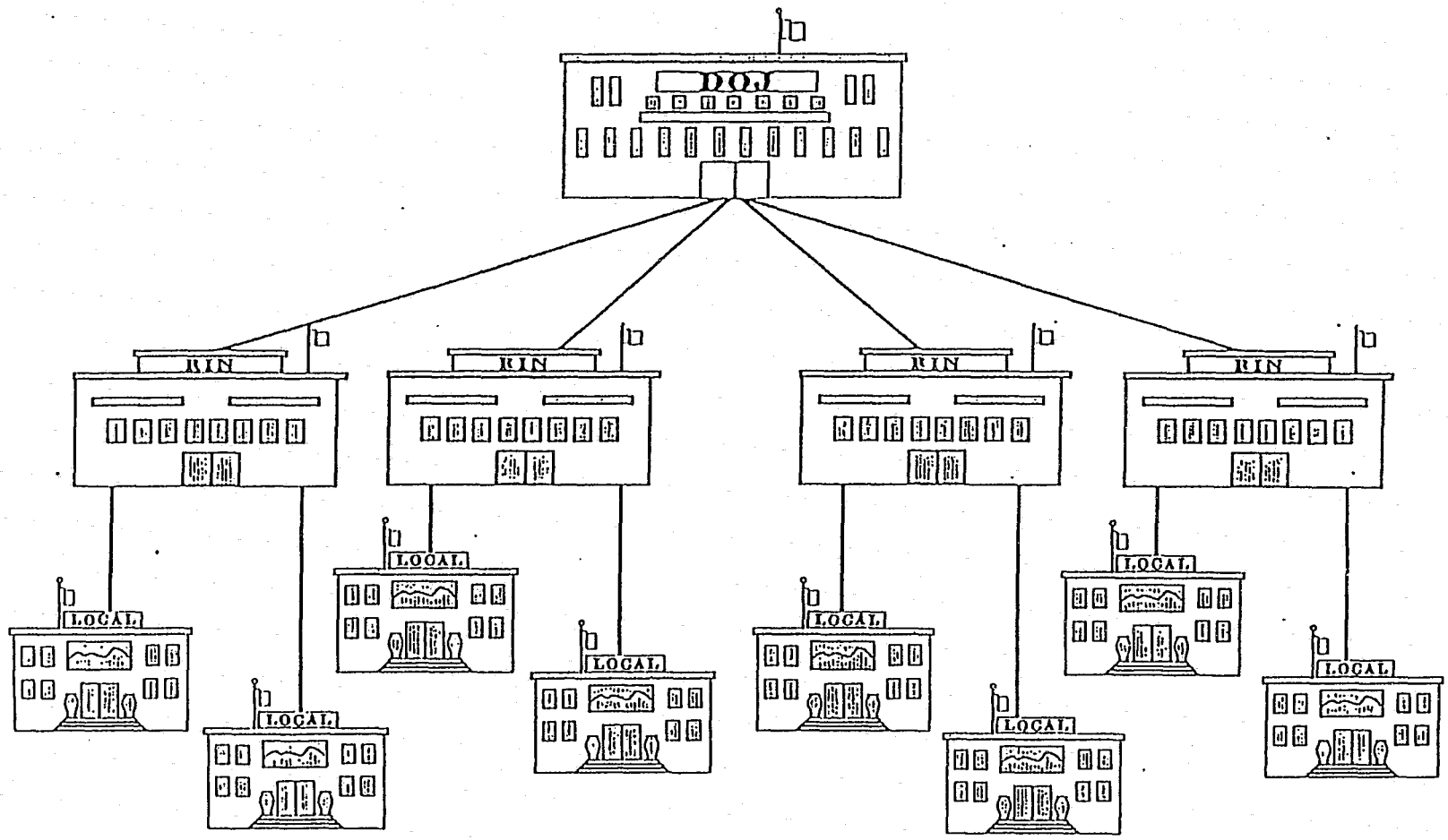
Figure 3 Centralized Network



DOJ = CALIFORNIA DEPARTMENT OF JUSTICE

11/9/89
E. COLLIN

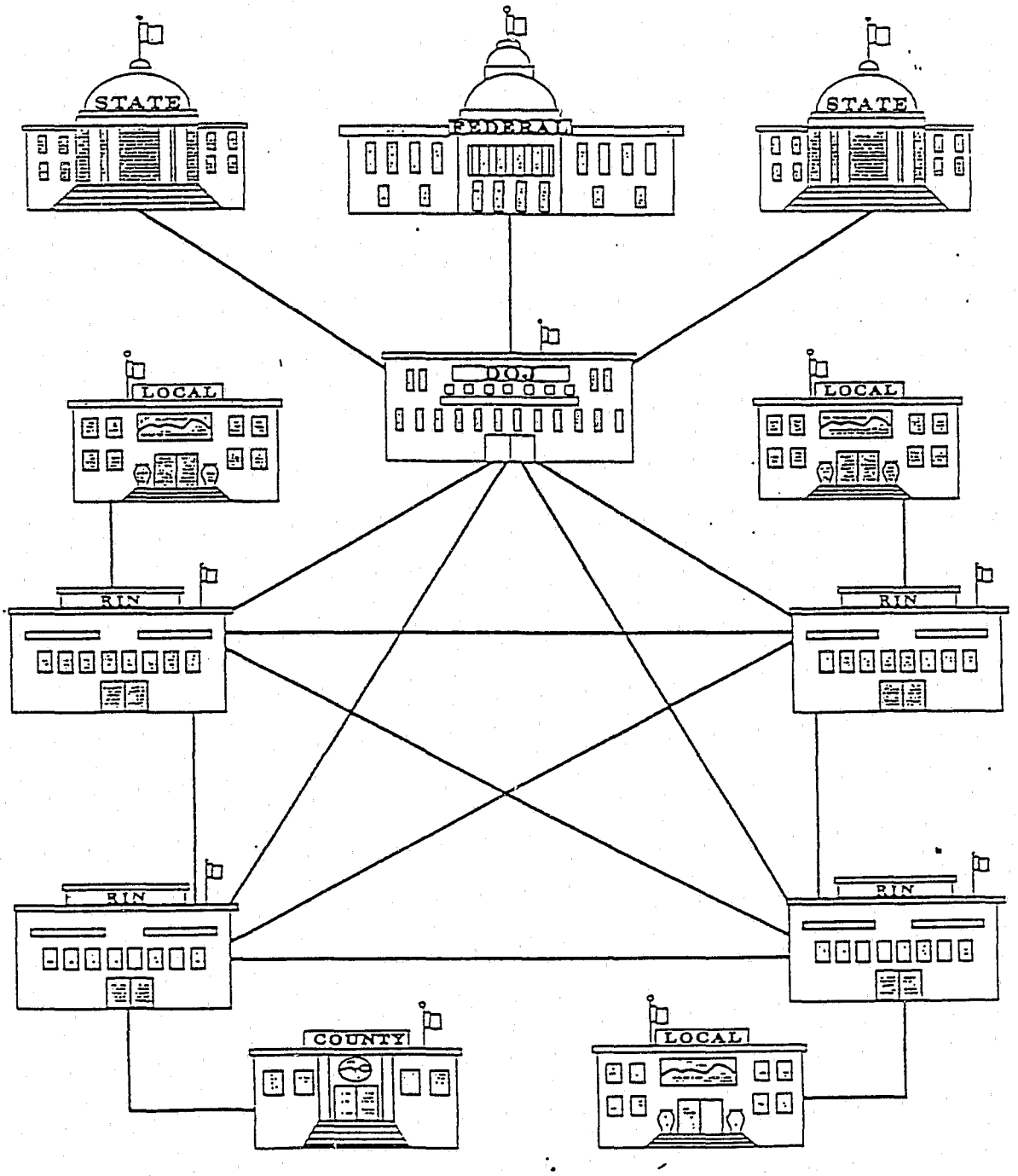
Figure 4 Hierarchical Network



DOJ = CALIFORNIA DEPARTMENT OF JUSTICE
RIN = REGIONAL IDENTIFICATION NETWORK / CAL-PHOTO

11/9/89
B. COLLIN

Figure 5 Decentralized Network



DOJ = CALIFORNIA DEPARTMENT OF JUSTICE
RIN = REGIONAL IDENTIFICATION NETWORK / CAL-PHOTO

11/9/89
E. COLLIN

Appendix D - Persons Interviewed

United States Secret Service
Institute for Law Enforcement Information Systems Management
John Vezeris, Executive Director

Robert B. Barnes, Consultant

SEARCH Group Incorporated
Bill Spernow

California Office of Criminal Justice Planning
Carol Berger, Senior Program Specialist

Department of Justice
Chuck Jones, Supervising Agent

Texas Tri-State Project
Ken Burkhalter

Alameda County Sheriff's Office
Lieutenant Bud Wilkinson, PIN Manager

Regional Career Criminal Apprehension Program
Bud Frank, Executive Director
Criminal Justice Council of Santa Cruz County

ARJIS (Automated Regional Justice Information System)
Nancy Angus, Manager
San Diego, California

California Department of Justice, Cal-Photo
Robert W. Drake

Department of Justice, Bureau of Organized Crime and Criminal Intelligence
Serious Habitual Offender Program
Rod Stinson, Director