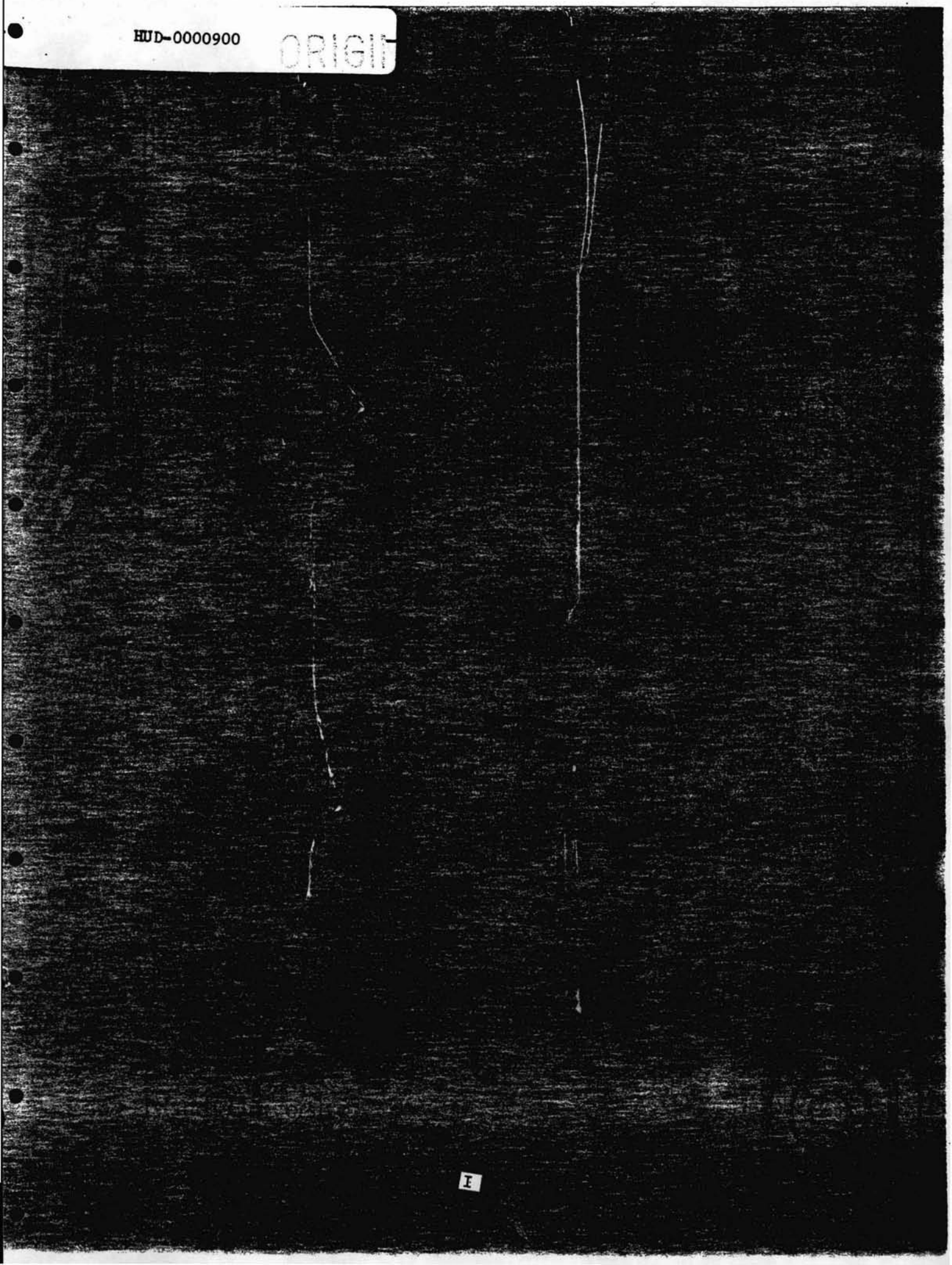

DATA PROCESSING DEDICATION: A USAC CONCERN

Municipal Systems Research Project

Claremont Men's College and Long Island University

Research Associates:

O. E. Dial
Carl F. Davis, Jr.
Eugene Kozik
Kenneth L. Kraemer
William H. Mitchel
Myron E. Weiner

II

"Research sponsored by the Office of
Policy Development and Research, U.S.
Department of Housing and Urban Development."

FOREWORD

This paper is one of a series dealing with USAC Programs and Areas of Concern. Papers tentatively being prepared in the series are:

USAC Programs

- USAC Concepts and Philosophy
- USAC Objectives
- Overview of USAC programs
- USAC Organization and Membership
- IMIS Program Status
- HRDS Prototype Program Specification

Areas of Concern

- Automation
- Integration
- Transferability
- Geocoding
- Data standardization
- File organization
- Data management
- Evaluation
- Costs and Benefits
- Intergovernmental data flows
- Dedicated Systems
- Confidentiality

DATA PROCESSING DEDICATION: A USAC CONCERN

What is the Issue

The FBI requires that systems participating in the NCIC-CCH network be dedicated to that exclusive purpose, and that EDP facilities be managed and controlled by criminal justice agencies.	vs.	USAC requires that the systems it is developing in cities be integrated in such a way that data bases, processess, and facilities are shared, consistent with the rules of data access control and with local conditions.

In Focus

USAC Position:- The USAC approach to Integrated Municipal Information Systems (IMIS) requires that the system be designed from a system-wide (municipal-wide) perspective; that the system be operated under centralized direction; that the data base and processes be integrated so as to facilitate data, process, and facility sharing, thereby minimizing redundancy and enhancing data availability; and that a data access control plan be instituted so as to ensure the confidentiality of the data base and the security of the system.

NCIC Position:- The National Crime Information Center (NCIC), operated by the Federal Bureau of Investigation, provides a computer based national criminal history index and network to states and selected metropolitan areas. Cities participate through their respective state or metropolitan area centers. Acting on the recommendations of the NCIC Advisory Policy Board, participants in the Computer Criminal History (CCH) portion of the system are required to dedicate any hardware, including terminals, to be operated exclusively by personnel of criminal justice agencies; and, similarly, to restrict access to the criminal history data base to those same personnel.

Impact:- The NCIC system through its related control terminals and the advent of criminal history, has a potential of over 45,000 local, state and Federal criminal justice user terminals. Since a large share of this potential includes targets for IMIS, it would appear that cities must make choices between IMIS or participation in the NCIC network. As the rules now stand, a city may not, with consistency, participate in both programs.

Example:-Project CLEAR operates a regional computer center which serves Cincinnati and Hamilton County, Ohio. The system is designed along USAC guidelines with respect to integration of the data base and data processing, and data access control measures. The facility, operating under the guidance of a Control Board, grants first priority to servicing the police information system in which some 43 police departments in the county as well as all court and corrections agencies participate. Second priority is granted to the development of the Hamilton County Information System and Cincinnati Information System.

The Regional Computer Center (RCC) has participated in the NCIC system since early in 1969 and has experienced significant benefits by doing so. This relationship was formalized to include CCH participation in agreement with the FBI on February 1, 1972. The agreement provides, inter alia, that "NCIC reserves the right to immediately suspend (participation in the system) when either the security or dissemination requirements approved by the NCIC Advisory Policy Board and adopted by the NCIC are violated."

In a hearing before the Confidentiality Committee of the NCIC Advisory Policy Board on June 14, 1972, it was established that, contrary to NCIC policy, RCC, at the request of the Hamilton County Police Association,

ran a Property Index System on the communications processor concurrently with the Police Information System. Further, that while management control was vested in a criminal justice agency, administrative control of tax levy funds supporting the operations included non-criminal justice people.

On June 26th, 1972, the RCC was advised that in the opinion of the Security and Confidentiality Committee, NCIC Advisory Policy Board, "the CLEAR system does not conform to the NCIC policy requirements relative to the handling of interstate criminal history information. RCC participation in the NCIC network subsequently was terminated by the FBI.

Background

LEAA and Project SEARCH:- The Law Enforcement Assistance Administration (LEAA) was established June 19, 1968, under the general authority of the Attorney General, to assist state and local governments in reducing crime, and improving their law enforcement and criminal justice systems. The principal operating divisions are the Office of Law Enforcement Programs, and the National Institute of Law Enforcement and Criminal Justice. It was the latter, in response to its mission of encouraging research and development to strengthen law enforcement, which recommended approval of project SEARCH for funding by LEAA.

SEARCH is an acronym for "System for Electronic Analysis and Retrieval of Criminal Histories". The project, with ten states initially participating, *was to address a requirement for a computerized national system for

---

*Project SEARCH was coordinated by the California Council on Criminal Justice through the California Crime Technological Research Foundation. The ten participating states are: Arizona, California, Connecticut, Florida, Maryland, Michigan, Minnesota, New York, Texas, and Washington. Five other states were in observer status: Colorado, Illinois, New Jersey, Ohio, and Pennsylvania.

exchanging criminal history data by the development of a prototype. SEARCH had two objectives to be accomplished during its projected 18-month project life (June 30, 1969--December 31, 1970):

> o Establish and demonstrate the feasibility of an on-line system allowing for the interstate exchange of offender history files based on a compatible criminal justice offender record, integrating basic information needs of police, prosecution, judicial and correctional agencies.
>
> o Design and demonstrate a computerized statistics system based on an accounting of individual offenders proceeding through the criminal justice system.

The Resulting Prototype: - The prototype which resulted from the research and which was subsequently implemented in selected states, was based on the maintenance of state-held files and the existence of a Central Index, directly accessible by each state, and containing summary data on each state-held file. The system provides that when a transaction takes place between an offender and an agency in a state other than the Agency of Record, the criminal history file is transferred from the previous Agency of Record, the file is updated, and the central index is updated to reflect these changes.

The normal flow of traffic in the network would originate with an inquiry from a local terminal to the state computer system, which in turn would be transmitted to the Central Index in Michigan. The Central Index would reply via the state with summary information including personal descriptors, identifying numbers, abbreviated criminal profile, and the name of the Agency of Record (state of agency holding the full criminal history record). The requesting agency would then query the Agency of Record via

the same network to the Agency of Record computer in order to receive the full criminal history record. Updates can only be transmitted to the Central Index by state-level agencies.*

Privacy and Security: - All sensitive public records, like other kinds of records, are subject to unintentional errors, misuse of data, and unauthorized data change. Project SEARCH was mainly interested, therefore, in discovering; (1) the degree to which the consequences of these problems were substantially different, and (2) the extent to which these problems would be more prevalent when a computer with its associated high-speed response and remote access capability was a part of the system.

SEARCH concluded that:

o With respect to unintentional errors--the recording and processing discipline associated with the use of a computer is likely to reduce the frequency of unintentional error. Many errors not caught are allowable to a manual system, but will inhibit the operation of a computer system. However, the consequences of some types of errors may be substantially amplified simply by the fact that there are many more persons with access and the system response speed may exceed the error detection and correction speed.

o With respect to misuse of data--the possibility that the data will be misused may increase substantially over a manual system because of the increase in users and the easy access, unless controls are implemented. The computer itself introduces more opportunities for misuse. For example, a computerized file can be quickly searched by whatever data elements it contains, such that the compilations of subjects can be prepared with respect to ceratain characteristics contained in the file.

o With respect to intentional modification of data--the opportunity for intentional modification or destruction of records is increased in proportion to the file centralization of the system.

* It is understood that a recent change in the system provides that the Center now files the full criminal history record as well.

> A disc or tape file is much more vulnerable to undetectable modifications by programming or other means than the more inefficient dispersed paper file.

Given these problems together with the probability that organized crime might attempt to penetrate the system for purposes of intentional modification of data, SEARCH undertook a program to address the security and privacy issues. This effort resulted in the preparation of a "Code of Ethics" (See Appendix 1), a set of procedures concerning security and privacy which were included in the SEARCH Operating Manual, and the creation of the Security and Privacy Committee. This committee was subsequently carried forward under the NCIC Advisory Board.

The currently effective NCIC provisions for Privacy and Security are contained in the NCIC "Background, Concept and Policy" statement of March 31, 1971. (The portion of this document relating to privacy and security are set forth in Appendix 2.) These provisions constitute an expansion of the Code of Ethics, primarily, and contain implementing provisions. Those extracts which impinge upon USAC's IMIS are as follows:

> o Criminal history records and other law enforcement operational files should not be centrally stored or controlled in "data bank" systems containing non-criminal justice related information.
>
> o Direct access (to data) . . .will be permitted only for criminal justice agencies.
>
> o All computers, electronic switches, and manual terminals interfaced directly with the NCIC computer . . .must be under the management control of criminal justice agencies authorized as control terminal agencies. Similarly, satellite computers and manual terminals accessing NCIC through a control terminal agency computer must be under the management control of a criminal justice agency. . . . Management control must remain fully independent of non-criminal justice data systems and criminal justice systems shall be primarily dedicated to the service of the criminal justice community. (Emphasis supplied)

o If law enforcement or other criminal justice agencies are to be responsible for the confidentiality of the information in computerized systems, then they must have complete management control of the hardware and the people who use and operate the system. (Note: Then why not the telephone companies whose lines are used in network communications, also.)

o Historically, law enforcement/criminal justice has been responsible for the confidentiality of its information. This responsiblilty cannot be assumed if its data base is in a computer system out of law enforcement/criminal justice control.

o The function of public safety and criminal justice demands the highest order of priority, 24 hours a day. Experience has shown that this priority is best achieved and maintained through dedicated systems.

o Historically, police and criminal justice information have not been intermingled or centrally stored with non-criminal social files, such as revenue, welfare, and medical, etc. This concept is even more valid with respect to computerized information systems at both national and state levels.

o Criminal history data . . .will be made available outside the Federal government only to criminal justice agencies for criminal justice purposes. This precludes the dissemination of such data for use in connection with licensing, local or state employment other than with a criminal justice agency, etc. There are no exceptions pending legislative action at state and Federal level or Attorney General regulations.

o The person's right to see and challenge the contents of his record shall form an integral part of the system with reasonable administrative procedures.

o Lines/channels being used to transmit criminal history information must be dedicated solely to criminal justice use.

Current Developments:- The foregiong is based upon material published by SEARCH, LEAA and NCIC. This discussion of current developments, on the other hand, is based upon conversation with Mr. John Plants, Chairman, Security and Confidentiality Committee of the NCIC Advisory Board, and Mr. Paul K. Wormeli, Vice President, Public Systems, Inc., copies of correspondence which have been circulated, and papers and speeches of persons who figure prominently

in this issue.

These sources indicate that a serious division exists between LEAA and the FBI over the matter of systems dedication. LEAA advocates a more moderate policy, one which takes account of local circumstances and state law in specifying system configuration and control. The end result of privacy, security and priority can be achieved by methods other than system dedication, they argue.

The FBI, on the other hand, is adamant in its position that systems dedication alone can achieve these ends in the degree of assurance that is required for the handling of sensitive files. The existing policy, having been challenged by LEAA, is now before the Attorney General for clarification.

USAC:- USAC, an acronym for Urban Information Systems Inter-Agency Committee, was created with representation from some ten Federal departments and agencies -- those having programs which impinged upon urban areas of the United States. One of the several functions of USAC is to serve as a coordinating mechanism in providing interagency and intergovernmental perspective and support for a program of urban information systems research and development.

The first program of USAC, Integrated Municipal Information Systems (IMIS), was begun in 1970 in six cities, five of which continue to participate in the program today. The uniqueness of the program is more easily understood by reference to the basic concepts which guide the developmental effort. They are:

- The processes of government are best interrelated through an integrated data processing system.
- Computers can be used effectively only after a fundamental analysis of the operations of government have been made, and those operations understood.
- The most expeditious and effective method for developing an IMIS is the systems approach.
- Routine information and decision processes should be automated.
- Design and development should exploit the full range of computer technology.
- The basic building blocks of intergovernmental information systems are local governments.
- In order to assure system maintenance and economic feasibility, the system must be operations-based.
- The system should be designed for transfer from one government to another, thus enabling other governments to by-pass much of the research and development phases.
- The designed system should be installed incrementally consistent with an overall systems plan.

It should be readily apparent that USAC seeks to improve the capability of local governments in the administration of their affairs through automation. But much more is implied. Perhaps of greatest significance is the possibility of restoring explicit relationships and communications between the departments and bureaus of local governments and the functions which they administer, thus overcoming the functional fragmentation which is characteristically a crucial problem in each city today.

This existing situation is further exacerbated by the Federal practice of designing single-function programs for urban areas. To take one example, defacto computer dedication can be the result of an HEW program providing funds to computerize the record keeping of a school system. IMIS requires

the participation of that school system in a city-wide, integrated information system, thus making school data available, subject to data access control rules, to other departments of the city which might benefit from its use. Similarly, data generated in other departments will be of use and available to the school system.

But it should readily be seen that dedication, whether explicit or de-facto, is in conflict with several of the concepts enumerated above, and would defeat the objectives of IMIS. Foremost of these is the requirement for the integration of the data base, data processing, and processing facilities.

Commentary:- USAC views NCIC as providing a critically important coordinating and information service to states and local communities. USAC also views the relationship of USAC project cities and NCIC as having complementary roles. Furthermore, USAC shares the concern of NCIC for privacy, security and priority. The point where USAC takes issue with NCIC is in the mechanics of implementing the NCIC philosophy and role. Specifically, USAC views the requirement for dedication at the local level as excessive, wasteful of resources, beyond the fiscal ability of many cities to support, contrary to the theme of integration which is central to the USAC approach to the design of information systems, and unessential towards the achievement of effective data access control.

In attempting to differentiate qualitative differences between criminal history files and such other files as cities might use in the administration of government, SEARCH makes a good case for regarding them very similar in terms of sensitivity, but very different with respect to the threat of penetration by organized crime which renders the necessity of absolute criminal

justice control. However, this would not appear to hold up when it is considered that local agencies participating in the NCIC network are not empowered to update, add or delete information (certainly the would-be primary object of organized crime penetration) from the Central Index. Only Agencies of Record (States) may do so. It would seem therefore that dedication, if required at all is most appropriate to the state agency and has little relevance to local agencies.

It would appear that project SEARCH has become the research and advisory arm of NCIC. The membership of SEARCH, primarily from state-level offices, explains the state-level orientation of NCIC policies, i.e., local jurisdictions may make inquiries only; state jurisdictions will maintain Agency of Record files; and only states may update NCIC files at the Central Index. Furthermore, there is reflected a singular absence of appreciation of the utility of files other than police derived files in the conduct of police work.

The NCIC determination to protect its system in terms of privacy and security must be viewed as admirable, but misguided to the extent that it operates in a vacuum, totally without regard for the extent or nature of its impingement upon other functions served by local governments, or upon other Federal agencies serving the interests of local governments. It is this aspect which points up the need for broader representation in its advisory structures. Specifically, the Advisory Board of NCIC should include local representation as well as state, and provide for USAC liaison.

During the same years that Project SEARCH and NCIC were developing and implementing a prototype, USAC, too, was occupied by similar efforts. But while SEARCH and NCIC operated in virtual isolation with respect to the function

it was serving, USAC attempted to structure a process of consultation which would ensure the presentation of views from every category of persons upon which its prototype would impinge. Perhaps the best evidence of this is the pre-organizational seminar conducted at URISA, the representation on the USAC Committee of every Federal Agency having programs which impacted the urban area, and the inclusion of such organizations as NLC/ICMA in its councils.

Curiously, USAC had even established the chain of consultation which presumably would have bridged and encouraged communications between NCIC and USAC, namely, by ensuring that the Department of Justice was represented on the USAC Committee. Conventionally, this member has been from LEAA, an agency which had a direct link to SEARCH, but virtually none with the FBI, and hence none with NCIC. But the SEARCH link was enough to alert USAC of impending conflict in the principles espoused by each, and of the need for timely negotiation.

The fact remains that NCIC was developed under one set of guiding principles--dedication--and USAC under another--sharing. If both programs are to survive, and certainly both have merit, each must strive to find the common ground of accommodation.

But it should be recognized that there are significant objections to the dedication aspect of the NCIC approach quite apart from USAC qua USAC considerations. While these are most appropriately dealt with in LEAA correspondence with the Attorney General, and hence are not to be recited here, there is one which must be made explicit and recognized as a basic threat to the fundamental freedoms which Americans enjoy. Because of the

magnitude of the threat it is considered appropriate for discussion in this paper.

Power is an inevitable by-product of an information system centralized at the national level. The exclusiveness of a system so designed would provide a direct, confidential communications link with criminal justice agencies in every jurisdiction and governmental level of the United States. While this has desirable features, the requisite auditing mechanism, one which would assure that the system were free from abuse, would consist solely of criminal justice representation, namely, the users of the system. This practice is not supported in American traditions of government.

This is not to imply that the FBI or NCIC would abuse the power generated by the system. But the unaudited capability is there. Hence, the system does not accord with sound business practice. The participation of elected officials at all jurisdictions in the auditing process is essential to an assurance that the system is free from abuse.

What is USAC Doing About It

USAC Project Cities

USAC Project cities have varying degrees of present involvement with LEAA and NCIC, or , are looking toward such involvement in the future. This involvement, particularly participation in the NCIC network, is encouraged as a matter of USAC policy. This outlook is facilitated by the more moderate data access control requirements of NCIC with respect to the use of those

files other than criminal history files, i.e., Wants and Warrants, Stolen Vehicles, Stolen Plates, etc. It is not facilitated by the requirement for system dedication, a prerequisite to participation in the Criminal History File.

In an effort to negotiate differences in approach, the Chairman, USAC, has met with the Chairman, Security and Confidentiality Committee of the NCIC Advisory Board. It was agreed as an outcome of that meeting that USAC representatives would study the soon-to-be-released NCIC Standards and Goals document in order to identify those standards which conflict with the USAC approach. The list of such items would then constitute the agenda of a further conference. The purpose of the conference would be the resolution of differences with respect to each item.

It is now apparent, however, that such a conference might be merely academic. It is doubtful that a recommendation of the Advisory Board itself would be sufficient to alter the position of the FBI in the matter of dedication.

What Further Action is Required

The USAC position with respect to negotiating differences with NCIC should be as follows:

- Delete the requirement for system dedication at the local level, assuming that the local level will continue to be limited to an inquiry capability.

- Delete the requirement at the local level that criminal history files cannot be processed with other files, i.e., property files, for police purposes.

o Ensure that data access control plans at the local level include measures which assure NCIC that the requisite level of protection is available for purposes of confidentiality and security.

o Ensure that local systems provide that level of priority required for participation in the NCIC network.

o Increase the membership of the Advisory Board of NCIC and appropriate committees of the board to include representation from USAC and selected local jurisdictions.

o Communicate with the Administrator, LEAA, to ensure that these USAC concerns are reflected in his position paper.

o Communicate these USAC concerns through the Secretary, HUD, to the Attorney General at the earliest possible time.

APPENDIX 1.

SEARCH
CODE OF ETHICS

Project SEARCH participants believe that a nationwide capability for quick access to offender criminal histories is essential for effective law enforcement and administration of criminal justice.

It is recognized, however, that the extraordinary increase in accessibility and responsiveness associated with the use of computer-based information systems may increase the possibility of unauthorized disclosure or misuse of the data in other than legitimate law enforcement and criminal justice functions. Therefore, in order to provide reasonable protection of individual privacy and to secure the data maintained in the System, the participants in Project SEARCH pledge to observe the following:

Article I. Limitations of the System

SECTION 1. Limited area of government. The participants should limit the area of concern to criminal justice as a matter of government function.
SECTION 2. Limited category of users. The participants should limit access to the System to criminal justice agencies who would assume responsibility for the legitimate criminal justice use of System data and provide penalties for improper disclosure. Rules governing access should be definite and subject to public scrutiny.
SECTION 3. Limited functions.

A. The participants should limit the role of the Central Index to an information service only.
B. The participants should limit the System, at the national level, to an index or directory role rather than a registry function.

SECTION 4. Limited information.

A. The participants should limit System records to certain subjects - those for whom arrest fingerprints have been recorded. The recording of data about an individual should be initiated only upon the report of a crime and the commencement of criminal justice system proceedings.
B. The participants should limit data collection to only that which is relevant for the criminal justice process. Thus, data about individuals such as contained in census, tax, election, unemployment insurance, and similar files should not be collected or accessed through the System.
C. The participants should specifically exclude from the System all unverified information such as informant-supplied data or intelligence data.

Article II. Integrity of Information

SECTION 1. Assurance of individual privacy. The participants should make a continuous effort to refine every step of the criminal justice information system provided by SEARCH to assure that the most sophisticated measures are employed and the most perceptive judgements are made in the development and operation of the System to optimize the protection of individual privacy.

SECTION 2. Collection and maintenance of data.

A. The participants should be greatly concerned with the completeness and accuracy of the information in the System. Regular auditing of the data bank should be undertaken to assure the reliability of stored data.

B. The participants should establish criteria for re-evaluation of the data contained in the System and for purging where deemed appropriate.

C. The participants should provide measures for purging from the Central Index the computerized file of the record of first offenders where criminal proceedings have resulted in a determination in favor of such persons.

D. The participants should encourage the provision of procedures for an individual to learn the contents of the arrest record kept about him and for the correction of inaccuracies or prejudicial omissions in a person's arrest record.

SECTION 3. Dissemination of data.

A. The participants should develop a classification sub-system to assure that sensitive data is provided premium security and that all data is accorded appropriate protection. Data should be disseminated to criminal justice agencies on a "need-to-know" basis.

B. The participants should make provisions in appropriate cases to limit the derogatory impact of arrest records by providing meaningful descriptions of the nature of a person's criminal act so that false conclusions concerning the character of the individual are avoided.

C. The participants should employ a high level of computer, legal, physical, information, communications, and personnel security methods to reduce the possibility of breaching the security of the System.

SECTION 4. Advisory committee. The participants should establish an advisory committee to provide policy direction for the System and to entertain complaints about alleged intrusions on individual privacy.

Article III. Use of Data Base for Research

SECTION 1. Commitment to privacy. Where research is conducted as an activity of the System or utilizing data contained in the System Data Bank, the participants should recognize and affirm the claim to private personality and have a positive commitment to respect it.

SECTION 2. Safeguarding anonymity.

A. In the conduct of research, participants should divorce the identification of the individual as fully and as effectively as possible from the data furnished and preserve anonymity by aggregating, coding, and other appropriate measures.

B. Participants should safeguard research data in every feasible and reasonable way, and destroy the identification of the individual with any portion of the data as soon as possible, consistent with the research objectives.

NATIONAL CRIME INFORMATION CENTER (NCIC)

COMPUTERIZED CRIMINAL HISTORY PROGRAM

BACKGROUND, CONCEPT AND POLICY

AS APPROVED MARCH 31, 1971

AND

AMENDED AUGUST 31, 1971

BY

NCIC ADVISORY POLICY BOARD

BACKGROUND AND CONCEPT

The development in 1971, of the computerized criminal history file as part of the operating NCIC system is a major step forward in making this system of optimum value to all agencies involved in the administration of criminal justice. It is felt pertinent at this time to restate established NCIC concepts and operating policies, as well as new steps necessary to place this new application in its proper perspective. Offender criminal history has always been regarded by NCIC as the basic file in a criminal justice information system. From the beginning of NCIC sensitivity of a criminal history file with its security and confidentiality considerations has always been recognized (Science and Technology Task Force Report, The President's Commission on Law Enforcement and Administration of Justice, 1967).

It is important to keep in mind the need to develop an offender criminal history exchange with the states that will rapidly gain the confidence of all users in terms of system integrity, accuracy, and completeness of file content. This type of discipline is necessary if a nationwide system employing the necessary standards is to succeed. This is an essential consideration during the record conversion stage even though available data is limited, and becomes an essential goal in an operating on-line system.

From its inception, the concept of NCIC has been to serve as a national index and network for 50 state law enforcement information systems. Thus, the NCIC does not, nor is it intended to, eliminate the needs for such systems at appropriate state and metropolitan levels, but complements these systems. The concept was built on varying levels and types of information in metropolitan area, state and national files. In such an overall system many thousands of duplicate indices in local, state and Federal agencies could be eliminated and all agencies share in centralized operational information from a minimum number of computer files. The purpose of centralization beyond economics is to contend with increasing criminal mobility and recidivism (criminal repeating). Computer and communications technology makes this possible and, in fact, demands this system concept.

Our way of life demands that local and state government retain their traditional responsibility over law enforcement. Computer and communications technology such as NCIC enhances local and state capability to preserve this tradition. The NCIC system places complete responsibility for all record entries on each agency--local, state or Federal. Likewise, clearance, modification and cancellation of these records are also the responsibility of the entering agency. Each record, for all practical purposes, remains the possession of the entering agency. However, each local and state agency in one state can immediately share information contributed by another agency in another state. This continuity of information greatly increases the capability of local and state agencies in working across state lines which have in the past been barriers to mutual state and local law enforcement efforts.

The NCIC system, which is the first use of computer/communications technology to link together local, state and Federal governments, established the

control terminal concept. In a national system, although the individual users are responsible for the accuracy, validity, and completeness of their record entries and their action decisions on positive responses to inquiries, more stringent controls with respect to system discipline are required. A control terminal on the NCIC system is a state agency or a large core city servicing statewide or metropolitan area users. These control terminals, rapidly becoming computer based, share the responsibility in the national network in monitoring system use, enforcing discipline and assuring system procedures and policies are met by all users. The NCIC system through its related control terminals and the advent of criminal history, has a potential of over 45,000 local, state and Federal criminal justice user terminals. Tradition, computer/communications technology, and the potential size of the NCIC network and its related state systems demand that its management reponsibility be shared with the states. To accomplish this objective an NCIC Working Committee and an Advisory Policy Board were established.

From the beginning, the NCIC system concept has been to encourage and develop strong central state information and communications services. Through mandatory reporting laws at the state level, essential centralized files can be established for both operational and administrative use. The administrative or statistical use of computer based files is a vital consideration. A state cannot make intelligent decisions about crime problems or criminal justice effectiveness unless it can statistically document the extent and nature of crime and the success or failure of the criminal justice system in its treatment of offenders. Thus, the planning of these systems must incorporate means of obtaining the necessary statistical data as a by-product of the operational information being processed on a day-to-day basis. This is particularly true with respect to the criminal history application.

Of further significance are the centralized police statistics programs (Uniform Crime Reports) now operating in 10 states whereby comparative crime statistics are furnished to the national level through a central state agency. This statistical data furnished to the FBI for national use is merely a by-product of a more detailed state program which is an integral part of state law enforcement information services.

Offender criminal history, i.e., the physical and numerical descriptors of an arrested person and the basic recorded actions of the criminal justice agencies with respect to the offender and the charge, is vital information in day-to-day criminal justice operations. FBI studies as published in Uniform Crime Reports have documented the extent of criminal repeating by the serious offender, i.e., an average criminal career of 10 years and 6 arrests. With respect to criminal mobility, about 70 percent of the rearrests (criminal repeating) will be within the same state. Therefore, an offender criminal history file in scope and use is essentially a state file and a state need.

There is, however, substantial interstate criminal mobility (25-30 percent) which requires sharing of information from state to state. There is no way to positively identify a first offender who will later commit a crime in another state. The approach then to a national index must be an empirical

judgment that all state offenders committing serious and other significant violations must be included in the national index. As in other aspects of the system, the determination of which criminal acts constitute serious or significant violations resides with each individual state. A national index is required to efficiently and effectively coordinate the exchange of criminal history among state and Federal jurisdictions and to contend with interstate criminal mobility.

The development of offender criminal history for interstate exchange required the establishment of standardized offense classifications, definitions, and data elements. Felony and misdemeanor definitions cannot be used in this approach because of the wide variation in state statutes. In fact, the definitions of a specific crime by state penal codes also vary widely. For full utility and intelligent decision-making, offender criminal history requires a common understanding of the terminology used to describe the criminal act and the criminal justice action.

Computerized offender criminal history must have the criminal fingerprint card taken at the time of arrest as the basic source document for all record entries and updates. This is necessary in order to preserve the personal identification integrity of the system. While the criminal history file in the NCIC system will be open to all law enforcement terminals for inquiry, only the state agency can enter and update a record. This provides for better control over the national file and its content. It relies on a central state identification function to eliminate duplications of records and provides the best statistical opportunity to link together multi-jurisdictional criminal history at local and county level.

Using the NCIC concept of centralized state information systems, another requirement is to change the flow of criminal fingerprint cards. Local and county contributors within a state must in an ultimate operational system forward criminal fingerprint cards to the FBI through the central state identification function. Where the state can make the identification with a prior print in file, it can take the necessary action in a computerized file without submission to the FBI. Where the state cannot make the identification, the fingerprint card must be submitted to the national identification file. Again, the system's concept is that a fingerprint card must be the source document for a record entry and update, but now it will be retained at the state or national level. This approach eliminates considerable duplication of effort in identifying fingerprint submissions, particularly criminal repeaters at state and national level. It will be the responsibility of each state to determine its own capability in regard to servicing intrastate criminal fingerprint cards. Whenever a state has determined that it is ready to assume processing all intrastate criminal fingerprint cards, the state agency will inform contributors within the state to forward all criminal fingerprint submissions to the state identification bureau, including those which were previously directed to the FBI, and will also so inform the FBI. Since the success of the system concept depends on this procedure all possible measures will be taken to assure compliance.

As pointed out earlier, the justification for a national index is to efficiently and effectively coordinate 50 state systems for offender criminal history exchange. The need is to identify the interstate mobile offender. FBI statistics indicate that about 70 percent of the offenders confine their activity to a single state. These may be described as single state offenders. Another 25 to 30 percent of the offenders commit crimes supported by fingerprint cards in two or more states. FBI statistics with respect to more serious violators indicate that on an average, one-third accumulate arrests in three or more states over a 6 to 9-year period. Offenders with arrests in two or more states may be described as multiple state offenders.

In either event sufficient data must be stored in the national index to provide all users, particularly those users who do not have the capability to fully participate in the beginning system, the information necessary to meet basic criminal justice needs.

In order for the system to truly become a national system, each state must create a fully operational computerized state criminal history capability within the state before July 1, 1975.

Although the present need for the criminal history file and the unequal development of state criminal justice systems dictate a simple initial index structure, the ultimate system should differentiate between "multiple state" and "single state" offenders with respect to the level of residency of detailed criminal history. "Single state" offenders would be those whose criminal justice interactions have been non-Federal and confined to a single state having a computerized criminal history system.

The interstate exchange of computerized criminal history records requires a standard set of data elements and standard definitions. The system design must be built upon user needs for all criminal justice agencies and end with user input. It should be designed on what it is possible to achieve in the future and initially operate on the information and hardware available at all levels at the present time. While the proposed formats and standardized offense classifications and definitions seem ambitious, to approach a system of this potential scope and size without a plan to substantially improve the identification/criminal history flow would be a serious error.

System Concept

As pointed out earlier the concept of NCIC since initial planning in 1966 has been to complement state and metropolitan area systems. Although computer/communications technology is a powerful tool, a single national file of detailed law enforcement data was viewed as being unmanageable and ineffective in serving the broad and specialized needs of local, state and Federal agencies. The potential size and scope of a national system of computerized criminal history involving 45,000 criminal justice agencies demands joint management by the states and the FBI/NCIC.

Necessity for State Files

(1) Seventy percent of the criminal history records will be single state in nature, i.e., all criminal activity limited to one state and, therefore, the responsibility of and of primary interest to that state.

(2) State centralization can tie together the frequent intrastate, multijurisdictional arrests of the same offender and thus eliminate unnecessary duplication of files at municipal and county level. This will obviously result in economies.

(3) A state system with a detailed data base, because of its manageable size, can best satisfy most local and state criminal justice agency information needs both on and off line. The national file then complements rather than duplicates the state file.

(4) A state with a central data base of criminal history has the necessary statistical information for overall planning and evaluation including specialized needs unrelated to the national file.

(5) State control of record entry and updating to national file more clearly fixes responsibility, offers greater accuracy, and more rapid development of the necessary standards.

(6) A central state system provides for shared management responsibility with FBI/NCIC in monitoring intrastate use of the NCIC, including security and confidentiality.

(7) By channeling the criminal identification flow through the state to the national level eliminates substantial duplication of effort at national and state levels.

Compatibility of State and National Files

(1) To contend with criminal repeating and mobility, a national index of state and Federal offender criminal history is necessary, i.e., a check of one central index rather than 51 other jurisdictions.

(2) The duplication does provide a backup to recreate either a national or state file in the event of a disaster, a crosscheck for accuracy, validity, and completeness as well as a more efficient use of the network.

(3) The NCIC record format and data elements for computerized criminal history afford a standard for interstate exchange.

(4) In the developed system single state records (seventy percent) will become an abbreviated criminal history record in the national index with switching capability for the states to obtain the detailed record. Such an abbreviated record should contain sufficient data to satisfy most inquiry needs, i.e., identification segment, originating agency, charge, data, disposition of each criterion offense and current status. This will substantially reduce storage costs and eliminate additional duplication.

Program Development

The proper development of the Computerized Criminal History Program, in terms of its impact on criminal justice efficiency and effectivenss and dollar costs, is vital. At the present time there is a wide range of underdevelopment among the states in essential services such as identification, information flow, i.e., court disposition reporting programs, computer systems and computer skills.

(1) NCIC will implement computerized criminal history in November, 1971, requiring the full interstate format for both single and multi-state records because:

(a) This enables all states to obtain the benefits of the Computerized Criminal History Program.
(b) This provides all states time to develop and implement the necessary related programs to fully participate.
(c) Familiarity with and adherence to all system standards speed program development.

(2) It is understood that the NCIC Computerized Criminal History Program will be continually evaluated, looking toward the implementation of single state, multi-state concept.

Levels of Paticipation

(1) State maintains central computerized criminal justice information system interfaced with NCIC. The state control terminal has converted an initial load of criminal history and these records are stored at state and national levels. The state control terminal has the on-line capability of entering new records into state and NCIC storage, as well as the ability to update the computer stored records. Through the state system local agencies can inquire on-line for criminal history at state and national levels. This is a fully participating NCIC state control terminal.

(2) State maintains an electronic switch linking local agencies for the purpose of administrative message traffic and on-line access to NCIC through a high-speed interface. No data storage at state level; however, criminal history records are stored in NCIC and new records entered and updated by the state control terminal from a manual interface to the electronic switch. The switch provides local agencies direct access to NCIC for criminal history summary information and other files.

(3) The state maintains manual terminal on low-speed line to NCIC. State control terminal services local agencies off-line, i.e., radio, teletype and telephone. Since volume of computerized criminal history is relatively small the state control terminal may convert criminal history records, enter and update these records in NCIC. No computer storage at state level.

Levels 2 and 3 are interim measures until such time as the state agency secures the necessary hardware to fully participate. At that time the state records stored in NCIC will be copied in machine form and returned to the originating state to implement the state system.

SECURITY AND CONFIDENTIALITY

I. Information in FBI/NCIC Interstate Criminal History Exchange System

A. Entries of criminal history data into the NCIC computer and updating of the computerized record will be accepted only from an authorized state or Federal criminal justice control terminal. Terminal devices in other criminal justice agencies will be limited to inquiries and responses thereto. An authorized state control terminal is defined as a state criminal justice agency on the NCIC system servicing statewide criminal justice users with respect to criminal history data. Control terminals in Federal agencies will be limited to those involved in the administration of criminal justice and/or having law enforcement responsibilities.

B. Data stored in the NCIC computer will include personal identification data, as well as public record data concerning each of the individual's major steps through the criminal justice process. A record concerning an individual will be initiated upon the first arrest of that individual for an offense meeting the criteria established for the national file. Each arrest will initiate a cycle in the record, which cycle will be complete upon the offender's discharge from the criminal justice process in disposition of that arrest.

C. Each cycle in an individual's record will be based upon fingerprint identification. Ultimately the criminal fingerprint card documenting this identification will be stored at the state level or in the case of a Federal offense, at the national level. At least one criminal fingerprint card must be in the files of the FBI Identification Division to support the computerized criminal history record in the national index.

D. The data with respect to current arrests entered in the national index will be restricted to serious and/or significant violations. Excluded from the national index will be juvenile offenders as defined by state law (unless the juvenile is tried in court as an adult); charges of drunkenness and/or vagrancy; certain public order offenses, i.e., disturbing the peace, curfew violations, loitering, false fire alarm; traffic violations (except data will be stored on warrants for manslaughter, driving under the influence of drugs or liquor, and "hit and run"); and non-specific charges of suspicion or investigation.

E. Data included in the system must be limited to that with the characteristics of public record, i.e.:

1. Recorded by officers of public agencies or divisions thereof directly and principally concerned with crime prevention, apprehension, adjudication or rehabilitation of offenders.

2. Recording must have been made in satisfaction of public duty.

3. The public duty must have been directly relevant to criminal justice responsibilities of the agency.

F. Social history data should not be contained in the interstate criminal history system, e.g., narcotic civil commitment or mental hygiene commitment. If, however, such commitments are part of the criminal justice process, then they should be part of the system.

Criminal history records and other law enforcement operational files should not be centrally stored or controlled in "data bank" systems containing non-criminal justice related information, e.g., welfare, hospital, education, revenue, voter registration, and other such non-criminal files necessary for an orderly process in a democratic society.

G. Each control terminal agency shall follow the law or practice of the state or, in the case of a Federal control terminal, the applicable Federal statute, with respect to purging/expunging data entered by that agency in the nationally stored data. Data may be purged or expunged only by the agency originally entering that data. If the offender's entire record stored at the national level originates with one control terminal and all cycles are purged/expunged by that agency, all information, including personal identification data will be removed from the computerized NCIC file.

II. Steps to Assure Accuracy of Stored Information

A. The FBI/NCIC and state control terminal agencies will make continuous checks on records being entered in the system to assure system standards and criteria are being met.

B. Control terminal agencies shall adopt a careful and permanent program of data verification including:

1. Systematic audits conducted to insure that files have been regularly and accurately updated.

2. Where errors or points of incompleteness are detected the control terminal shall take immediate action to correct or complete the NCIC record as well as its own state record.

III. Who May Have Access To Criminal History Data

A. Direct access, meaning the ability to access the NCIC computerized file by means of a terminal device, will be permitted only for criminal justice agencies in the discharge of their official, mandated responsibilities. Agencies that will be permitted direct access to NCIC criminal history data include:

1. Police forces and departments at all governmental levels that are responsible for enforcement of general criminal laws. This should be understood to include highway patrols and similar agencies.

2. Prosecutive agencies and departments at all governmental levels.

3. Courts at all governmental levels with a criminal or equivalent jurisdiction.

4. Correction departments at all government levels, including corrective institutions and probation departments.

5. Parole commissions and agencies at all governmental levels.

6. Agencies at all government levels which have as a principal function the collection and provision of fingerprint identification information.

IV. Control of Criminal Justice Systems

All computers, electronic switches and manual terminals interfaced directly with the NCIC computer for the interstate exchange of criminal history information must be under the management control of criminal justice agencies authorized as control terminal agencies. Similarly, satellite computers and manual terminals accessing NCIC through a control terminal agency computer must be under the management control of a criminal justice agency. Management control is defined as that applied by a criminal justice agency with the authority to employ and discharge personnel, as well as to set and enforce policy concerning computer operations. Management control includes, but is not limited to, the direct supervision of equipment, systems design, programming and operating procedures necessary for the development and implementation of the computerized criminal history program. Management control must remain fully independent of non-criminal justice data systems and criminal justice systems shall be primarily dedicated to the service of the criminal justice community.

The Board endorses the following statement by the Director of the FBI before the Subcommittee on Constitutional Rights of March 17, 1971. "If law enforcement or other criminal justice agencies are to be responsible for the confidentiality of the information in computerized systems, then they must have complete management control of the hard-

ware and the people who use and operate the system. These information systems should be limited to the function of serving the criminal justice community at all levels of government---local, state and Federal."

The following are considerations:

1. Success of law enforcement/criminal justice depends first on its manpower, adequacy and quality, and secondly, information properly processed, retrievable when needed and used for decision making. Law enforcement can no more give up control of its information than it can its manpower.

2. Computerized information systems are made up of a number of integral parts, namely, the users, the operating staff, computers and related hardware, communications and terminal devices. For effectiveness, management control of the entire system cannot be divided between functional and nonfunctional agencies. Likewise, the long-standing law enforcement fingerprint identification process is an essential element in the criminal justice system.

3. Historically, law enforcement/criminal justice has been responsible for the confidentiality of its information. This responsibility cannot be assumed if its data base is in a computer system out of law enforcement/criminal justice control.

4. The function of public safety and criminal justice demands the highest order of priority, 24 hours a day. Experience has shown that this priority is best achieved and maintained through dedicated systems.

5. A national/statewide public safety and criminal justice computer/communications system, because of priority, scope including system discipline, and information needs, on and off line, will require full service of hardware and operating personnel.

6. Historically, police and criminal justice information have not been intermingled or centrally stored with non-criminal social files, such as revenue, welfare, and medical, etc. This concept is even more valid with respect to computerized information systems at both national and state levels.

7. These systems, particularly public safety and criminal justice information systems, must be functional and user oriented if they are to develop effectively. Computer skills are a part of the system. Ineffective systems result not only in the greatest dollar loss but also costs in lives.

V. Use of System-Derived Criminal History Data

A. Criminal history data on an individual from tbe national computerized file will be made availabe outside the Federal government only to criminal justice agencies for criminal justice purposes. This precludes the dissemination of such data for use in connection with licensing, local or state employment other than with a criminal justice agency, etc. There are not exceptions pending legislative action at state and Federal level or Attorney General regulations.

B. The use of data for research should acknowledge a fundamental commitment to respect individual privacy interests with the identification of subjects divorced as fully as possible from the data. Proposed programs must be reviewed by the NCIC or control terminal agency to assure their propriety and to determine that proper security is being provided. All non-criminal justice agency requests involving the identities of individuals in conjunction with their national criminal history records must be approved by the Advisory Policy Board.

The NCIC or control terminal agency must retain rights to monitor any research project approved and to terminate same if a violation of the above principles is detected. Research data shall be provided off line only.

C. Should any information be verified that any agency has received criminal history information and has disclosed that information to an unauthorized source, immediate action will be taken by NCIC to discontinue criminal history service to that agency, through the control terminal if appropriate, until the situation is corrected.

D. Agencies should be instructed that their rights to direct access encompass only requests reasonably connected with their criminal justice responsibilities.

E. The FBI/NCIC and control terminals will make checks, as necessary, concerning inquiries made of the system to detect possible misuse.

F. The establishing of adequate state and Federal criminal penalties for misuse of criminal history data is endorsed.

G. Detailed computerized criminal history printouts shall contain caveats to the effect, "This response based on numeric identifier only" and "Official use only - arrest data based on fingerprint identification by submitting agency or FBI." These caveats will be generated by the FBI/NCIC or state control terminal's computer or may be preprinted on paper stock.

VI. Right to Challenge Record

The person's right to see and challenge the contents of his record shall form an integral part of the system with reasonable administrative procedures.

VII. Physical, Technical, and Personnel Security Measures

The following security measures are the minimum to be adopted by all criminal justice agencies having access to the NCIC Compterized Criminal History File. These measures are designed to prevent unauthorized access to the system data and/or unauthorized use of data obtained from the computerized file.

A. Computer Centers

1. The criminal justice agency computer site must have adequate physical security to protect against any unauthorized personnel gaining access to the computer equipment or to any of the stored data.

2. Since personnel at these computer centers can access data stored in the system, they must be screened thoroughly under the authority and supervision of an NCIC control terminal agency. (This authority and supervision may be delegated to responsible criminal justice agency personnel in the case of a satellite computer center being serviced through a state control terminal agency.) This screening will also apply to non-criminal justice maintenance or technical personnel.

3. All visitors to these computer centers must be accompanied by staff personnel at all times.

4. Computers having access to the NCIC must have the proper computer instructions written and other built-in controls to prevent criminal history data from being accessible to any terminals other than authorized terminals.

5. Computers having access to the NCIC must maintain a record of all transactions against the criminal history file in the same manner the NCIC computer logs all transactions. The NCIC identifies each specific agency entering or receiving information and maintains a record of those transactions. This transaction record must be monitored and reviewed on a regular basis to detect any possible misuse of criminal history data.

6. Each state control terminal shall build its data system around a central computer, through which each inquiry must pass for screening and verification. The configuration and operation of the center shall provide for the integrity of the data base.

B. Communications

1. Lines/channels being used to transmit criminal history information must be dedicated solely to criminal justice use, i.e., there must be no terminals belonging to agencies outside the criminal justice system sharing these lines/channels.

2. Physical security of the lines/channels must be protected to guard against clandestine devices being utilized to intercept or inject system traffic.

C. Terminal Devices Having Access to NCIC

1. All agencies having terminals on the system must be required to physically place these terminals in secure locations within the authorized agency.

2. The agencies having terminals with access to criminal history must have terminal operators screened and restrict access to the terminal to a minimum number of authorized employees.

3. Copies of criminal history data obtained from terminal devices must be afforded security to prevent any unauthorized access to or use of that data.

4. All remote terminals on NCIC Computerized Criminal History will maintain a hard copy of computerized criminal history inquiries with notation of individual making request for record (90 days).

VIII. Permanent Committee on Security and Confidentiality

A permanent committee has been established, composed of NCIC participants, which group will address the problems of security and privacy on a continuing basis and provide guidance to the NCIC Advisory Policy Board. Some areas recommended for study are:

A. The consideration of criteria for the purging of records, i.e., deletion of records after a designated period of criminal inactivity or attainment of a specified age, etc.

B. The consideration of criteria for qualification of non-criminal justice agencies for secondary access to criminal history data.

C. A model state statute for protecting and controlling data in any future system should be drafted and its adoption encouraged.

IX. Organization and Administration

A. Each control terminal agency shall sign a written agreement with the NCIC to conform with system policy before participation in the criminal history program is permitted. This would allow for control over the data and give assurance of system security.

B. In each state the control terminal agency shall prepare and execute a written agreement containing similar provisions to the agreement by the states and NCIC with each criminal justice agency having a terminal device capable of accessing criminal history data within that state.

C. Each state criminal justice control terminal agency is responsible for the security throughout the system being serviced by that agency, including all places where terminal devices are located.

D. A system security officer shall be designated in each control terminal agency to assure all necessary physical, personnel, computer and communications safeguards prescribed by the Advisory Policy Board are functioning properly in systems operations.

E. The rules and procedures governing direct terminal access to criminal history data shall apply equally to all participants in the system, including the Federal and state control terminal agencies, and criminal justice agencies having access to the data stored in the system.

F. All control terminal agencies and other criminal justice agencies having direct access to computerized criminal history data from the system shall permit an inspection team appointed by the Security and Confidentiality Committee to conduct appropriate inquiries with regard to any allegations received by the Committee of security violations. The inspection team shall include at least one representative of the FBI/NCIC. All results of the investigation conducted shall be reported to the Advisory Policy Board with appropriate recommendations.

G. Any non-compliance with these measures shall be brought to the immediate attention of the Committee which shall make appropriate recommendations to the Advisory Policy Board. This Board has the responsibility for recommending action, including the discontinuing or service to enforce compliance with system security regulations.

IMPORTANT ASPECTS OF NCIC CRIMINAL HISTORY BACKGROUND CONCEPT AND POLICY

BACKGROUND AND CONCEPT

Page 20 Para. 1

.....A control terminal on the NCIC system is a state agency or a LARGE CORE CITY servicing statewide or metropolitan area users. These control terminals, rapidly becoming computer based, share the responsibility in the national network in monitoring system use, enforcing discipline and assuring system procedures and policies are met by all users.....

Para. 2

.....Thus, the planning of these systems must incorporate means of obtaining the necessary statistical data as a by-product of the operational information being processed on a day-to-day basis. This is particularly true with respect to the criminal history application.

Page 21 Para. 3

Computerized offender criminal history must have the criminal fingerprint card taken at the time of arrest as the basic source document for all record entries and updates.

Page 22 Para. 3

In order for the system to truly become a national system, each state must create a fully operational computerized state criminal history capability within the state before July 1, 1975.

(This amounts to a license or directive to channel LEAA money for state preparation of NCIC policy.)

Page 23

(5) State control of record entry and updating to national file more clearly fixes responsibility, offers greater accuracy, and more rapid development of the necessary standards,

Program Development

Page 24 Para. 2

.....At the present time there is a wide range of underdevelopment among the states in essential services such as identification, information flow, i.e., court disposition reporting programs, computer systems and computer skills.

SECURITY AND CONFIDENTIALITY

Page 26 I. A. Entries of criminal history data into the NCIC computer and updating of the computerized record will be accepted only from an authorized state or Federal criminal justice control terminal. .....

(This is a deviation from the identification of a control terminal as identified on page 21.)

Page 27 II. A. The FBI/NCIC and state control terminal agencies will make continuous checks on records being entered in the system to assure system standards and criteria are being met.

Page 28 IV. All computers, electronic switches and manual terminals interfaced directly with the NCIC computer for the interstate exchange of criminal history information must be under the management control of criminal justice agencies authorized as control terminal agencies. Similarly, satellite computers and manual terminals accessing NCIC through a control terminal agency computer must be under the management control of a criminal justice agency..... .....Management control must remain fully independent of non-criminal justice data systems and criminal justice systems shall be PRIMARILY dedicated to the service of the criminal justice community.

Page 31 VII. Physical, Technical, and Personnel Security Measures

A. 1. The criminal justice agency computer site must have adequate physical security to protect against any unauthorized personnel gaining access to the computer equipment or to any of the stored data.

2. Since PERSONNEL AT THESE COMPUTER CENTERS CAN ACCESS DATA-STORED IN THE SYSTEM, THEY MUST BE SCREENED THOROUGHLY UNDER THE AUTHORITY AND SUPERVISION OF AN NCIC CONTROL TERMINAL AGENCY. (This authority and supervision may be delegated to responsible criminal justice agency personnel in the case of a satellite computer center being serviced through a state control terminal agency.) This screening will also apply to non-criminal justice maintenance or technical personnel.

Page 32 5. Computers having access to the NCIC must maintain a record of all transactions against the criminal history file in the same manner the NCIC COMPUTER LOGS ALL TRANSACTIONS.

(LEADS cannot comply with this regulation without significant software changes.)