National Crime Information Center

COMPUTERIZED CRIMINAL HISTORY PROGRAM

Background, Concept and Policy

APPROVED BY THE NCIC
ADVISORY POLICY BOARD
OCTOBER 20, 1976

FBI/DOJ

BACKGROUND AND CONCEPT

The establishment in 1971 of the Computerized Criminal History (CCH) File as part of the operating NCIC system was a major step forward in making this system of optimum value to all agencies involved in the administration of criminal justice. 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. Such discipline 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 need 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 governments 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, and 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 state-wide or metropolitan area users. These control terminals, rapidly becoming computer based, share the responsibility in the national network for 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 responsibility be shared with the states. To accomplish this objective, an NCIC Advisory Policy Board was 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 byproduct of the operational information being processed on a day-to-day basis. This is particularly true with respect to the criminal history application.

Of additional significance is a standardized law enforcement statistics program entitled "Uniform Crime Reports." Historically, this program collected crime statistics

directly from individual law enforcement agencies. For several years the program has embarked on an effort to assist the various states in creating their own statistical program. As of 1976, there were 36 states collecting crime statistics through a central state collection agency. The state programs provide the FBI with the necessary information to compile a national view of crime.

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. An FBI study entitled "Careers in Crime," published annually through the Uniform Crime Reporting Program, documents on a limited basis the extent of criminal repeating by the serious offender. Recent analysis indicates the number of years between the first and last (most recent) arrest was five years and five months and that within that time span the criminal repeater, measured on the basis of arrest, was arrested four times. A further study indicates 49 percent of persons arrested more than once were rearrested within the same state. When individuals having only one arrest are considered, then 67 percent of all the persons arrested were arrested within a single 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 (33 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.

Each computerized offender criminal history cycle must have a criminal fingerprint card as its basic source document. 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 criminal justice terminals for inquiry, only the state agency can enter and update a record. This procedure provides for better control over the national file and its contents. It relies on a central state identification function to eliminate duplication of records and provides the best statistical opportunity to link together multijurisdictional criminal history at local and county levels.

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 levels. 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 to the state identification bureau all criminal fingerprint submissions, 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 with respect to more serious offenders indicate that about 67 percent confine their criminal activity to a single state. These are categorized as single-state offenders. Therefore, 33 percent commit crimes, are arrested, and are fingerprinted in two or more states. These are categorized 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 state computerized criminal history capability within the state.

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 are 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 was built upon user needs for all criminal justice agencies and ends with user input. It was designed on what it is possible to achieve in the future, but to operate on the information and hardware available at all levels at the present time. While the formats and standardized offense classifications and definitions seem ambitious, to implement a system of this potential scope and size without a design 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 histories involving 45,000 criminal justice agencies demand joint management by the states and the FBI NCIC.

Necessity for State Files

(1) Sixty-seven 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 levels. 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 the national file more clearly fixes responsibility, offers greater accuracy, and brings about 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) 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 provides 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 a single-state record (67 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, date, 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 effectiveness 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 implemented computerized criminal history in November 1971, requiring the full interstate format for both single and multistate 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 will speed program development.

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

Levels of Participation

(1) The state maintains a central computerized criminal justice information system interfaced with NCIC. 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) The 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 is stored at state level; however, criminal history records are stored in NCIC and new records are 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 a manual terminal on low-speed line to NCIC. The state control terminal services local agencies off-line, i.e., via radio, teletype and telephone. Since the volume of computerized criminal history is relatively small, the state control terminal may convert criminal history records, enter and update these records in NCIC. There is 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 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 arrests for manslaughter, driving under the influence of drugs or liquor, and "hit and run"); and nonspecific 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 an integral part of a central data base containing noncriminal justice related information, e.g., welfare, hospital, education, revenue, and other such noncriminal 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 Access Criminal History Data

A. Direct access, meaning the ability to access the NCIC computerized file, will be permitted only under the management control of 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 governmental levels which have as a principal function the collection and provision of fingerprint identification information.

7. State control terminal agencies which have as a sole function by statute the development and operation of a criminal justice information system.

8. Regional or local governmental organizations established pursuant to statute which have as their sole function the collection and processing of criminal justice information and whose policy and governing boards have, as a minimum, a majority composition of members representing criminal justice agencies.

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. 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 the authority to set and enforce (1) priorities; (2) standards for the selection, supervision, and termination of personnel; and (3) policy governing the operation of computers used to process criminal history record information insofar as the equipment is used to process, store, or transmit criminal history record information. Management control includes, but is not limited to, the supervision of equipment, systems design, programming, and operating procedures necessary for the development and implementation of the computerized criminal history program. Such management control guarantees the priority service needed by the criminal justice community. A criminal justice agency must have a written agreement with the noncriminal justice agency operating the data center assuring that the criminal justice agency has management control as defined above.

The Board continues to endorse the following statement by the Director of the FBI before the Subcommittee on Constitutional Rights on 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 hardware 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."

Although dedication is not required for NCIC CCH participation, the security of the information contained in a criminal record system and the priority service needed by the criminal justice community will be enhanced by compliance with the following concepts:

1. Success of law enforcement/criminal justice depends first on its manpower, adequacy and quality, and secondly, on 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. Likewise, the long-standing law enforcement fingerprint identification process is an essential element in the criminal justice system.

3. Traditionally, 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. Traditionally, police and criminal justice information has not been intermingled or centrally stored with noncriminal 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 the national computerized file will be made available to Federal agencies authorized under Executive Order or Federal statute and to criminal justice agencies for criminal justice purposes. This precludes the dissemination of such data for use in connection with licensing or local or state employment, other than with a criminal justice agency or for other uses unless such dissemination is pursuant to Federal or state statutes. Such state laws may not conflict with Federal law. There are no exceptions.

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 noncriminal 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.

If an individual has a criminal record supported by fingerprints and that record has been entered in the NCIC CCH File, it is available to that individual for review, upon presentation of appropriate identification, and in accordance with applicable state and Federal administrative and statutory regulations.

Appropriate identification includes being fingerprinted for the purpose of ensuring that he is the individual that he purports to be. The record on file will then be verified as his through comparison of fingerprints.

A. Procedure

1. All requests for review must be made by the subject of his record through a law enforcement agency which has access to the NCIC CCH File. That agency within statutory or regulatory limits can require additional identification to assist in securing a positive identification.

2. If the cooperating law enforcement agency can make an identification with fingerprints previously taken which are on file locally and if the FBI Identification Number of the individual's record is available to that agency, it can make an on-line inquiry of NCIC to obtain his record on-line or, if it does not have suitable equipment to obtain an on-line response, obtain the record by mail. The individual will then be afforded the opportunity to see that record.

3. Should the cooperating law enforcement agency not have the individual's fingerprints on file locally, it is necessary for that agency to relate his prints to an existing record by having his identification prints compared with those already on file in the FBI or, possibly, in the State's central identification agency.

4. The subject of the requested record shall ask the appropriate arresting agency, court, or correctional agency to initiate action necessary to correct any stated inaccuracy in his record or provide the information needed to make the record complete.

VII. Physical, Technical, and Personnel Security Measures

The following security measures are the minimum to be adopted by all agencies having access to the NCIC Computerized 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 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 noncriminal 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

The communication circuits utilized to transmit criminal history information must be used solely by criminal justice agencies; i.e., there must be no terminals belonging to agencies outside the criminal justice system sharing these circuits.

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 criminal justice representatives, which group will address the problems of security, confidentiality, 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 noncriminal 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 to 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 of security violations received by the Committee. 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 noncompliance with these measures shall be brought to the immediate attention of the Committee which shall make appropriate recommendation to the Advisory Policy Board. This Board has the responsibility for recommending action, including the discontinuing of service to enforce compliance with system security regulations.

END