PRIVACY
AND
SECURITY PLANNING
INSTRUCTIONS

JUNE 30, 1975

LAW ENFORCEMENT ASSISTANCE ADMINISTRATION
U.S. DEPARTMENT OF JUSTICE

PREFACE

These instructions have been prepared to provide clarification and explanation of the Department of Justice Rules and Regulations governing criminal justice information systems. The instructions are intended to assist the agency in each State which is designated as being responsible for the State plan covering privacy and security, as well as other agencies which are affected by the regulations, in understanding the impact of the regulations and in preparing the State plan.

The materials contained herein do not have the same force of law as the regulations. However, this report has been thoroughly reviewed by the LEAA staff which will be responsible for approving State plans, and has the approval of LEAA. All discussions of policy issues are consistent with the regulations.

The instructions were prepared by Public Systems incorporated, Sunnyvale, California.

CONTENTS

CONTENTS (Continued)

Regulations Reference

Section 1

THE PLANNING PROCESS

On May 20, 1975, the Department of Justice issued Rules and Regulations governing data contained in criminal justice information systems. These regulations call for the preparation of a State plan and submission to LEAA for approval by December 16, 1975.

The purpose of these explanatory materials is to assist the States in the preparation of these plans. The materials contained herein are not to be construed as formal guidelines or requirements, but it is hoped that the information will clarify the intent and purpose of the Department in issuing these regulations.

RESPONSIBILITY FOR PLAN PREPARATION

The regulations require each State to prepare and submit to LEAA a criminal history record information plan. The purpose of the plan is to set forth operational procedures to guarantee the security and privacy of criminal history record information in systems funded by LEAA.

The Governor of each State is responsible for determining who shall be responsible for preparation of the plan. LEAA has requested each Governor to designate a responsible agency.

The regulations require that the designated State agency will be submitting a plan on behalf of the State. That is, the plan will have to address means for implementation of the regulations throughout the State. It is not envisioned that a plan will be submitted by each local and State agency maintaining criminal history record information. Rather, the single State plan will address the intentions of both State and local agencies in complying with the regulations.

There are obvious difficulties in this approach. A State agency cannot commit all State and local agencies to following the proposed procedures. However, many of the provisions address procedures to be instituted at the State level, such as at the central repository for criminal history record information. It is assumed that the agency which submits the plan 20.21(a)(1)

Regulations Reference

will be attesting to the acceptance of all the elements of the plan by the concerned State agencies. With respect to local systems that may come under the regulations, it is expected that the planning agency will base its certificate of compliance, which must be submitted with the plan, on certification provided by the local agencies. Further details on the certification process are given in Section 3.

It is also expected that the plan will indicate that the appropriate State agency will take steps to inform all agencies of procedures which will satisfy the regulations. Where other State or local agency systems are interfaced with or use data contained in the State central repository, these informational instructions will be implemented by means of contractual agreements. Should there be systems at a local level which are not a user of the State repository, the State is obligated to provide guidance in procedures for compliance as part of the certification process.

The formality of the intrastate review and approval process is a matter of discretion for each State. No particular process is required. States, however, are encouraged to involve State agencies such as: legislative bodies, State Planning Agencies, Statistical Analysis Centers, OBTS/CCH Data Centers, Offices of Attorney General, Judicial Conferences, Correctional Administrations, Departments of Public Safety, Bureaus of Identification, and local agencies including police, courts, corrections and other criminal justice-related agencies. The mechanisms for securing such involvement include: formal sign-offs or approvals by specific agencies, written comments from interested agencies, public hearings, and conferences or workshops.

AGENCIES COVERED BY THE REGULATIONS

All State and local agencies receiving LEAA monies after July 1, 1973 for manual or automated systems which collect, store, or disseminate criminal history record information are subject to these regulations. The regulations apply to criminal history record information collected at any time (either before or after July 1, 1973) unless specific provisions of the regulations indicate otherwise. Both criminal justice and non-criminal justice agencies may be subject to the regulations.

Regulations Reference 20.20(a)

The regulations do not apply to agencies which have received LEAA funds for general purposes other than the collection, storage or dissemination of criminal history record information. For example, an agency receiving funds to implement and operate automated non-criminal history record information systems (e.g., personnel, resource allocation, performance evaluation) would not by such fundings be included under the regulations.

The regulations also do not apply to agencies receiving criminal history record information from LEAA funded agencies unless the receiving agencies themselves have been granted LEAA funds for the collection, storage and dissemination of criminal history information, or the receiving agencies by contract expressly agree to be subject to the regulations.

In other words, the mere receipt of criminal history record information by Agency B from Agency A does not bring Agency B within the scope of these regulations, even if Agency A's system is federally funded. If, however, Agency B received criminal history record information under a contract with Agency A in which B agreed to be bound by the provisions of the regulations, the regulations would thereafter apply in toto to Agency B. (See the section on Dissemination in these instructions for further discussion.)

TIMING AND THE PLANNING PROCESS

Each State is required to submit its plan by December 16, 1975. The principal phases of each State's planning process will be drafting, review by appropriate agencies, and the actual submission of the plan.

Within 90 days of the receipt of the plan, LEAA shall approve or disapprove the adequacy of the provisions of the plan. Evaluation of the plan by LEAA will be based upon whether the procedures set forth will accomplish the objectives of the regulations. Any plan which is disapproved will be returned to the State with written comments explaining its deficiencies. Should LEAA disapprove a plan, the State in question would have up to 90 days to prepare an adequate plan. (See Section 4 of these instructions for further discussion.) 20.23

After such a 90-day extension, LEAA may apply fund cutoff procedures authorized by Section 509 of the Omnibus Crime Control and Safe Streets Act, as implemented by 28C.f.r. Part 18.

KEY CONCEPTS IN THE PLANNING PROCESS

Criminal Justice Agency

The regulations repeatedly refer to special requirements applicable only to criminal justice agencies. It is vital, therefore, to understand the meaning of "criminal justice agency" and "administration of criminal justice."

Regulations Reference

20.3(c)

"Criminal justice agency means: (1) courts; (2) a government agency or any subunit thereof which performs the administration of criminal justice pursuant to a statute or executive order, and which allocates a substantial part of its annual budget to the administration of criminal justice."

20.3(d)

"The administration of criminal justice means performance of any of the following activities: detection, apprehension, detention, pretrial release, post-trial release, prosecution, adjudication, correctional supervision, or rehabilitation of accused persons or criminal offenders. The administration of criminal justice shall include criminal identification activities and the collection, storage, and dissemination of criminal history record information."

An affirmative answer to each of the following questions is required for an agency to be considered a criminal justice agency:

1) Is the agency a "government agency" or a subunit thereof?

   To be characterized as "governmental," the head of the agency in question must be administratively responsible to elected public officials or to persons appointed by elected public officials. In addition, the specific agency or the specific subunit thereof must be authorized by statute or executive order to perform one of the functions of the administration of criminal justice. Corporations and other private agencies which by contract perform important functions related to criminal justice should not be considered as government agencies.

20.25

   The requirement for authority based on a statute or executive order will require some State and local agencies covered by the regulations to seek such authority. It was not the intent of the regulations to cause a disruption of services now being provided to criminal justice because of this restriction. Instead, it should be noted that most of the regulations do not have to be implemented until December 31, 1977. Thus, agencies should have time to acquire the necessary authority.

2) Is the agency performing one of the specific functions of the administration of justice (e.g., detection, apprehension) pursuant to a Federal or State statute or executive order?

   Language in the statute or executive order must expressly indicate that the agency is authorized to perform a function of the administration of criminal justice.

3) Does the agency or subunit thereof (if it is not a court) allocate a substantial part of its annual budget to the administration of criminal justice?

It is difficult to define an exact percentage for the term "substantial," and it is also obviously arbitrary to select a specific number. It nevertheless appears that "substantial" means more than 50% of the annual budget. However, the variety of accounting or budgeting procedures which may be used to compute such a figure make it necessary to examine carefully the purpose of this test before making final decisions. The commentary on the regulations indicates that any agency or subunit which is to be construed as a criminal justice agency under these regulations should have as its principal function one of the functions of the administration of criminal justice as defined in the regulations. This should not be taken as requiring that such an agency be exclusively performing administration of criminal justice functions.

Included as criminal justice agencies would be traditional police, courts, and corrections agencies as well as subunits of non-criminal justice agencies performing a function of the administration of criminal justice pursuant to Federal or State

statute or executive order. The above "subunit of non-criminal justice agencies" could include, for example, investigative offices of the U. S. Department of Agriculture which has as a major function the collection of evidence for criminal prosecutions of fraud. It is also possible for a functional subunit of a data processing agency to qualify as a criminal justice agency under these regulations.

The level in the organization defined to be a criminal justice agency must be construed narrowly if the intent of the regulations is to be met. State legislators, governors, State criminal justice planning agencies, city administrators and mayors, heads of non-criminal justice departments and their immediate assistants may generally exercise oversight and supervision of criminal justice subunits in the course of their many duties. Under normal circumstances, general policy-makers and purely staff agencies such as those mentioned above are not to be considered as criminal justice agencies.

The general rule is that agencies and individuals which provide only funding, oversight, staff services, general supervision, or policy guidance without regularly engaging in the day-to-day management or administration of criminal justice activities (detection, apprehension, etc.) are not criminal justice agencies under the regulations.

In exceptional cases, a chief administrator may assume decision-making powers reserved to traditional criminal justice officials. In these specific circumstances, an informal decision may require access to criminal history record information. The disseminating agency or subunit under such circumstances has the burden of determining whether the facts warrant considering the chief executive as a part of a criminal justice agency. These situations are expected to be infrequent.

Criminal History Record Information

The regulations apply only to criminal history record information. Agencies which do not collect, store, or disseminate criminal history record information are not subject to the regulations. The definition presented in the regulation states that "Criminal history record information means information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, informations, or other formal criminal charges, and any

20.3(b)

disposition arising therefrom, sentencing, correctional supervision, and release. The term does not include identification information such as fingerprint records or photographs to the extent that such information does not indicate involvement of the individual in the criminal justice system."

As a practical matter, criminal history files can only be effectively established when they are based on fingerprints. Therefore, criminal history record information means only information related to offenses in connection with which an individual's fingerprints were taken. Where arrests are made without taking fingerprints, such as in traffic offenses and minor infractions, information on the arrests and subsequent dispositions are not criminal history record information.

The definition of criminal history record information is intended to include the basic offender-based transaction statistics/computerized criminal history (OBTS/CCH) data elements. If notations of an arrest, disposition, or other formal criminal justice transactions occur in records other than the traditional "rap sheet" such as arrest reports, any criminal history record information contained in such reports comes under the definition of this subsection.

However, the definition does not extend to other information contained in criminal justice agency reports. Intelligence or investigative information (e.g., suspected criminal activity, associates, hangouts, financial information, ownership of property and vehicles) is not included in the definition of criminal history information.

The definition also does not extend to information such as statistics derived from offender-based transaction statistics systems which do not reveal the identity of individuals. Criminal records of corporations are not included in the definition of criminal history record information since identifiable individuals are not involved.

Various criminal justice information systems such as subject-in-process, prosecution management and inmate records systems contain data on arrests and other criminal justice system transactions. The regulations apply to these and other such systems containing criminal history record information, subject to six specific exceptions.

20.20

Regulations Reference

20.20(b)

The regulations do not apply to information contained in:

(1) Posters, announcements, or lists for identifying or apprehending fugitives or wanted persons.

(2) Original records of entry such as police blotters maintained by criminal justice agencies, compiled chronologically and required by law or long-standing custom to be made public, if such records are accessed on a chronological basis.

(3) Court records of public judicial proceedings compiled chronologically. This exception covers both manual files and automated files, if such files are solely within the management and control of a court system.

The exception does not apply where management and control of court-contributed information is shared with other agencies or vested in another separate agency.

(4) Published court opinions or public judicial proceedings.

(5) Record of traffic offenses maintained by State departments of transportation, motor vehicles or the equivalent thereof for the purpose of regulating the issuance, suspension, revocation, or renewal of driver's, pilot's or other operators' licenses.

(6) Announcements of executive clemency.

In item (2) above, original records of entry include police and other criminal justice agency records which traditionally have been used to give the public direct access to information relating to the identity of persons under the supervision of a criminal justice agency.

An example of an original record of entry is a police blotter, arrest book, or other equivalent record in which the fact of arrest is entered manually once a subject is in custody and which is customarily made available to the press for inspection.

20.20(b)(2)

The major function of such records is to provide current information on police activity and to guard

Regulations Reference

against secret arrests. The difficulty of retrieval of arrest information from chronological original records of entry such as the traditional police blotter tends to discourage unwarranted inquiries into a person's past record. For all of the above reasons, the regulations do not apply to such records.

Where original records of entry are not maintained, the regulations nonetheless recognize that announcements of ongoing developments in the criminal justice process should not be precluded from public disclosure. Thus, announcements of arrest, convictions, new developments in the course of an investigation may be made within a few days of their occurrence.

It is also permissible for a criminal justice agency to confirm certain matters of public record information upon specific inquiry. Thus, if a question is raised: "Was X arrested by your agency on or around Christmas time, 1952?" and this can be confirmed or denied by looking at an original record of entry, then the criminal justice agency may respond to the inquiry.

In many areas the blotter has been eliminated in favor of computerized booking systems. In some local jurisdictions, it has been possible for private individuals and/or newsmen upon submission of a specific name to obtain, through a computer search, a history of a person's arrests. Such files create a partial criminal history data bank potentially damaging to individual privacy, especially since they do not contain final dispositions. For the purposes of the exception set forth in section 20.20(b)(2), such systems can now only be accessed on a chronological basis.

Indeed, manual systems keyed to specific individuals which contain all of the agency's arrest reports compiled over a period of time have the same potential for abuse as computerized systems. By requiring that such records be accessed solely on a chronological basis, the regulations limit inquiries to specific time periods and discourage general fishing expeditions into a person's private life. It is the specific intent of these regulations to prohibit wholesale disclosures of an individual's arrest history.

Regulations Reference

Section 2

ELEMENTS OF A CRIMINAL HISTORY RECORD INFORMATION PLAN

This part sets forth instructions for development and implementation of the criminal history record information plan specified in the regulations which require each State to submit a plan setting forth "operational procedures" to implement the provisions of this section of the regulations. — 20.21

It should be emphasized that the plan must provide for full compliance in every respect with the requirements and limitations set forth in Section 20.21. However, pursuant to Sections 20.22 and 20.23, not all of the procedures set out in the plan need be fully implemented at the time the plan is submitted. Section 20.22 requires that the procedures for access and review by record subjects set out in Section 20.21(g) must be fully operational upon plan submission. All other provisions in the plan should be implemented to the "maximum extent feasible." This is stated by the regulations to mean that all provisions must be implemented that do not require additional legislative authority, involve unreasonable cost or exceed existing technical ability at the time of plan submission. — 20.22(a)

If these latter factors require delayed implementation of specific provisions, the certification required by the regulations must identify these procedures, state the degree of implementation achieved at the time of plan submission and describe the steps being taken to overcome the barriers that have prevented full implementation. — 20.22(b)(3)

All procedures in the plan must be fully operational by December 31, 1977, except that implementation of the computer hardware dedication requirement may be delayed by LEAA upon good cause shown. Thus, to comply with the regulations, each State must (1) devise a plan providing for full compliance with Section 20.21; (2) determine the extent to which full implementation of the procedures set out in the plan will require additional legislation, additional funds or additional technology; (3) take steps to overcome these barriers; and (4) devise a schedule of implementation designed to achieve full operation of all plan procedures as soon as feasible and in any event by December 31, 1977. — 20.23 — 20.21(f)(2)

Regulations Reference

The State plan should contain four major sections:

1. Objectives of the Plan
2. Approach to Achieving the Objectives
3. Schedule of Major Milestones
4. Responsibilities of Involved Agencies.

Each section should present the intent of the State in complying with the regulations.

LEAA does not anticipate receiving large documents in this planning process. As mentioned in the commentary, these plans should be considerably less than the detail contained in, for example, State Comprehensive Plans. As a rule of thumb, the criminal history information plan should be between 50 and 75 single-spaced typewritten pages, not including the certifications of all covered agencies in the State, which may be supplied as an appendix to the plan.

Most of the material contained in these instructions deals with Section 2 of the plan--Approach to Achieving Objectives. The section on schedule should show specific time tables and major milestones in bringing agencies into compliance with the regulations. The milestones should reflect implementation dates for all operational procedures required by the regulations, in each of the five areas discussed here.

The last section of the plan should specify the agencies having responsibility for implementation of the required procedures, including all of the various different responses the State will make to comply with the regulations. For example, if the plan calls for legislative action, an agency should be assigned the responsibility of drafting legislation.

The remainder of this part of the instructions includes a brief discussion of objectives and a discussion of the operational procedures and actions required to comply with the regulations. States should feel free to use as much of this material as they wish in writing their own plans.

Regulations Reference

OBJECTIVES

Section 524(b) of the Omnibus Crime Control and Safe Streets Act provides--

> "(b) All criminal history information collected, stored, or disseminated through support under this title shall contain, to the maximum extent feasible, disposition as well as arrest data where arrest data is included therein. The collection, storage, and dissemination of such information shall take place under procedures reasonably designed to insure that all such information is kept current therein; the Administration shall assure that the security and privacy of all information is adequately provided for and that information shall only be used for law enforcement and criminal justice and other lawful purposes. In addition, an individual who believes that criminal history information concerning him contained in an automated system is inaccurate, incomplete, or maintained in violation of this title, shall, upon satisfactory verification of his identity, be entitled to review such information and to obtain a copy of it for the purpose of challenge or correction."

To implement this provision, the regulation provides that each State plan must set forth operational procedures on: (a) completeness and accuracy, (b) limitations on dissemination, (c) general policies on use and dissemination (relating to non-criminal justice purposes), (d) juvenile records, (e) audit, (f) security, and (g) access and review. The guidelines follow this format, except that (b), (c) and (d) are grouped under one heading on limits on dissemination. 20.21

Completeness and Accuracy

Each plan must set forth procedures to insure that criminal history record information is complete and accurate. "Complete" means, in general, that arrest records should show all subsequent dispositions as the case moves through the various segments of the criminal justice system. The approach of the regulations is that complete records "should" be maintained at a central State repository, and the minimum 20.21(a)(1)

completeness requirements included in the regulations are made applicable to records maintained at such central repositories. "Accurate" means containing no erroneous information of a material nature. The regulations require operational procedures to minimize the possibility of erroneous information storage and a system for notification of prior recipients when erroneous information is discovered.

Limits on Dissemination

As noted above, Section 524(b) of the Safe Streets Act requires that dissemination and use of criminal history record information be limited to "criminal justice and other lawful purposes." The regulations require each State plan to contain operational procedures relating to dissemination for criminal justice purposes and for such non-criminal justice purposes as licensing, employment checks, security clearances and research. The regulations also require procedures for responding to court orders or rules relating to the release of criminal history record information, and for limiting the dissemination of juvenile records for non-criminal justice purposes.

Audits and Quality Control — 20.21(e)

Inherent in Section 524(b) of the Omnibus Crime Control and Safe Streets Act is the requirement that criminal justice agencies devise some method for monitoring compliance with restrictions set out in the legislation. The regulations address this problem by requiring that appropriate records be kept of record disseminations and that each State conduct an annual audit of a representative sample of State and local criminal justice agencies to verify adherence to the regulations. The guidelines discuss the kinds of records that should be kept and the mechanics of the annual audit requirement.

Security — 20.21(f)

Section 524(b) requires that the security of criminal history record information be adequately provided for. The regulations set forth in some detail the procedures that must be instituted to implement this requirement, including procedures relating to hardware dedication, protection of physical facilities, and selection, training and supervision of employees.

Regulations Reference

Individual Right of Access and Review

One of the most effective ways to relieve the concern of many people about the kinds of information maintained in criminal justice information systems and at the same time help to insure the accuracy and completeness of the information is to permit the individual to review information maintained about him and to challenge and correct it if he deems it inaccurate or incomplete. Thus, Section 524(b) guarantees this right. The regulations set out in some detail the kinds of procedures that must be established to implement it. Included are procedures for access and review, administrative review and appeal of criminal justice agency actions, notifying prior recipients whenever information is corrected and advising the individual of the identity of non-criminal justice agencies that have received errorneous information about him. — 20.21(g)

The remainder of this section addresses the operational procedures required in each of the five major areas of the regulations.

COMPLETENESS AND ACCURACY

Section 524(b) of the Safe Streets Act requires that criminal history record information be kept current and that disposition data be included with arrest data to the maximum extent feasible. Thus, the regulations require the establishment of procedures for the prompt reporting of dispositions and for queries to insure that criminal justice agencies use and disseminate the most current data available. — 20.21(a)(1)

State Central Repositories

Clearly, the most effective, efficient and economical way of satisfying both of these requirements is through the establishment of a central State repository to serve all criminal justice agencies in the State, requiring the prompt reporting of all dispositions to this repository, and requiring all criminal justice agencies in the State to query the repository before disseminating criminal history record information to make sure the information is the most current available. Inquiries of a central State repository shall be made prior to any dissemination except in those cases where time is of the essence and the repository is technically incapable of responding within the necessary time period. Although the regulations do not strictly mandate this approach, they clearly recognize it as the most

appropriate. It greatly simplifies the problem of disposition reporting and eliminates the need for maintaining expensive duplicate complete criminal histories at the local level. Thus, States should adopt this approach in their plans unless there are compelling reasons for not doing so.

Establishment of Central State Repositories. The commentary defines a central State repository as "a State agency having the function pursuant to statute or executive order of maintaining comprehensive statewide criminal history record information files." The commentary further notes the expectation that "ultimately, through automatic data processing, the State level will have the capability to handle all requests for in-State criminal history information."

States should, therefore, seek legislative authority, where it does not already exist, creating a central repository of criminal history record information. The repository should have the authority by statute to maintain complete criminal history files available to criminal justice agencies throughout the State. It should have the capacity, supported by necessary automated data processing equipment and telecommunications and terminal facilities, to provide criminal identification and criminal history record services to all criminal justice agencies in the State.

Reporting of Dispositions. As noted, Section 524(b) of the Safe Streets Act requires that dispositions be included with arrests "to the maximum extent feasible." Thus, the plan must set forth procedures designed to insure reasonably prompt reporting of dispositions. Since it is expected that all States already have or will establish central State repositories for the maintenance of complete criminal histories, the regulations set minimum standards for reporting of dispositions to these central repositories. As a minimum, the plan must establish procedures to insure that all dispositions occurring within the State are reported to the central State repository within 90 days after occurrence for inclusion on arrest records available for dissemination.

"Disposition" is defined to include the formal conclusion of each stage of a case as it moves from arrest through the criminal justice system. The term includes police dispositions such as decisions not to refer charges; prosecutor dispositions such as elections not to commence criminal proceedings or to indefinitely postpone them; court dispositions such as convictions, dismissals, acquittals and sentences; 20.3(e)

corrections dispositions such as paroles or releases from supervision; and such other dispositions as pardons or executive clemency or appellate court decisions reversing or modifying earlier dispositions. To be complete under the regulations, a criminal history record must include all dispositions that have occurred in the case from arrest to final release of the individual from the cognizance of any segment of the criminal justice system. Thus, an effective disposition reporting system must include provisions for reporting of dispositions by every component of the system: police, prosecutors, courts and corrections.

To accomplish this, every State that does not already have such a law should seek legislation providing for mandatory reporting of dispositions. The legislation should require that dispositions be reported to the central State repository and should be binding on all components of the criminal justice system in the States at whatever level. The legislation should contain sufficient sanctions, including fines, penalties and audits, to assure that it is enforceable.

It should be noted that reporting need not be directly to the central repository. The legislation in some States conceivably will call for reporting to a local- or State-level collection point which will forward data to the central repository. For example, in some States the trial courts will be reporting to a judicial administration unit at the State level, which acts as a satellite data collection center for the central repository. There will also be instances where regional data systems will act as collection centers for local agencies, creating a subsequent interface to the central repository. These systems are quite useful and can assist the central repository in ensuring that reporting is complete.

Until such legislation can be obtained in States that do not have mandatory reporting laws, procedures must be established in the plans to insure disposition reporting to the maximum extent possible. These procedures should be supported by formal agreements between criminal justice agencies, identifying the officials in particular agencies who are responsible for disposition reporting. The procedures should require reporting to the central State repository (either directly or indirectly), which should have the responsibility for assuring that the procedures are being implemented.

Regulations Reference

The regulations call for the development of a system of reporting which records all dispositions. The disposition reporting system outlined in the plan should provide for the positive identification of an individual through fingerprint identification as well as the capability to uniquely track the individual through final disposition of the charges incident to the arrest. Care should be taken to insure that identification procedures established under the arrest and disposition reporting system are consistent with the national single-print submission concept, which calls for only the initial set of prints to be submitted to the FBI, and all subsequent submissions to be handled by the central State repository. All disposition information related to a specific arrest should be tied back to the set of fingerprints taken relative to the arrest via a tracking number or equivalent means of linking information generated by different agencies in the criminal justice process.

For example, an arrest and disposition reporting tracking number could be assigned at the time that the fingerprints are generated in the jail booking process. The tracking number would accompany forms or computer input formats which would follow the individual's case through prosecutor, courts, and correctional processing. Initial identification and arrest segment information as defined by the NCIC computerized criminal history system would immediately be submitted to the State repository along with the arrest and disposition tracking number, to facilitate tracking of all transactions subsequent to arrest.

As another example, a tracking number could also be assigned at the point that the complaint is issued. This tracking number could then be transferred onto the warrant commitment as well as the jail booking documentation, prosecution, courts, and correctional disposition reporting formats. Each tracking number would be unique to the individual and the charges related to the initial complaint. The positive identification process in this example would be accomplished at jail/booking (i.e., at the point when the tracking number previously established is entered onto the fingerprint card).

Disposition reporting forms or formats in both examples would be sent to the applicable criminal justice agencies which would submit appropriate disposition information to the State repository or to a satellite collection center. These two examples identify two of the many possible methods for disposition reporting. States are encouraged to create

Regulations Reference

reporting systems which best meet their own needs, within the bounds of these regulations.

Promptness of Disposition Reporting. The regulations provide that, in States that have central State repositories, dispositions occurring anywhere within the State must be reported to the repository within 90 days after occurrence. The regulations make this requirement applicable to "all arrests occurring subsequent to the effective date of these regulations." Thus, the 90-day limit is applicable only to arrests occurring after June 19, 1975. Dispositions relating to arrests made prior to that date are not subject to the limit even if the dispositions occur after that date. Such dispositions are, however, bound to be reported as promptly as possible under prevailing circumstances. Moreover, even with respect to arrests that occur after June 19, 1975, the 90-day period should be considered a minimum requirement. Every State plan should provide for the reporting of dispositions as promptly as feasible considering the existing state of development of criminal justice systems in the State. 20.21(a)(1)

Even though the regulations stipulate that dispositions should be submitted relative to arrests after June 19, 1975, there is language in the Act and the regulations to indicate that disposition reporting should be implemented "to the maximum extent feasible." The approach to be taken in complying should be aimed at creating a disposition reporting system if one does not already exist. There was no intent to require that agencies go back into the records and obtain dispositions for all arrests occurring before a disposition reporting system is in effect. Although agencies must pursue the development of disposition reporting in good faith, these procedures can be implemented as late as December 31, 1977. Where no implementation is possible now, agencies would not be expected to attempt to reconstruct records, even if the arrest occurred after June 19, 1975. 20.21(a)(1) 20.23

The plan should include some method of insuring implementation of the 90-day reporting requirement or whatever reporting requirement the plan provides. As a minimum, this must include a procedure for regular and random audits to check on conformance with reporting periods. The plan should detail this procedure, including a description of the audits to be performed, the individuals or agencies responsible for performing them and sanctions to be applied in the case of discovered violations. The detail provisions of audit procedures are discussed further in the section concerning audit and quality control. 20.21(e)

Regulations Reference

In addition, States may wish to consider including in their plans a procedure for some level of investigation before disseminating a record if no disposition has been recorded for a period long enough that a disposition can normally be expected to have occurred. Thus, a record of an arrest for a given offense with no disposition recorded might call for a check back before dissemination after a period of six months if court dispositions for that offense normally occur in four to five months and dispositions normally are reported within a week.

The extent to which procedures of this kind can be instituted, and, of course, the applicable time periods and the steps that can be taken to determine whether unreported dispositions have occurred, will vary greatly from State to State. However, each State should consider including some such procedure in its plans. As a minimum, even in States where reporting of dispositions is in an early stage of development and where criminal history record systems are almost entirely manual, the State should be able to implement a procedure of checking by telephone before disseminating arrest records over a year old to be sure that no disposition has occurred and that the case is still actively pending. The regulations require such a procedure to be established to prevent the dissemination of year-old arrest records for certain non-criminal justice purposes. Even though not required by the regulations, it would constitute sound record-keeping practice to also update records sent to criminal justice agencies where the disposition can be determined.

20.21(c)(1)

Query of Central Repository Before Dissemination. The regulations provide that, in those States that have central State repositories, "procedures shall be established for criminal justice agencies to query the central repository prior to dissemination of any criminal history record information to assure that the most up-to-date disposition data is being used." The regulations exempt from this requirement "those cases where time is of the essence and the repository is technically incapable of responding within the necessary time period." Although the commentary on this provision acknowledges that the presently existing central State repositories, which are for the most part manual, probably are incapable of meeting many "rapid access needs of police and prosecutors," such repositories can respond quickly enough for most non-criminal justice purposes and queries "can and should" be made before dissemination of records for such purposes.

20.21(a)(1)

Regulations Reference

The regulations require that queries be made prior to dissemination of criminal history records. Thus, the requirement is applicable where a police agency proposes to disseminate a record to another police agency or to a prosecutor's office. But it is not applicable, for example, where the record is transferred from one person to another within the same criminal justice agency.

The plan should set out in detail the procedures that will be implemented to comply with this requirement. The procedures should include formal agreements between the central repositories and user agencies, binding the users to make inquiries before further dissemination when feasible.

The plan should specify the instances when queries are required and when they may be dispensed with. These exceptions should be specified in terms of the purposes of dissemination and the response time requirements that might justify dissemination without querying the central repository. For example, if a given State's central repository is incapable of responding in less than 8 hours to a request for a criminal history, then the procedures might appropriately exempt from the query requirement enumerated disseminations, such as policy disseminations to prosecutors for arraignment or bail setting, for which 8 hours would not be an adequate response time. When disseminations of this kind are for the purpose of processing a charge through the criminal justice system and it is clear under the circumstances that no disposition has occurred, no query will be required, so long as the information disseminated relates only to the charge in process.

It should be stressed that the regulations are designed to implement a statutory provision that requires that criminal history records be kept current as to dispositions "to the maximum extent feasible." Thus, the intent is that every State shall endeavor to establish procedures to ensure that queries are made of central repositories before any dissemination of a criminal history record. Although exceptions are permitted in recognition of the reality that present manual repositories cannot respond quickly enough in every instance, these exceptions should be understood to apply only until central State repositories can be upgraded to a level of technical capability that will enable them to respond in a reasonable time for every query. It is expected that all central State repositories ultimately will employ sufficient automated data

Regulations Reference

processing equipment to be able to serve all of the information needs of criminal justice agencies throughout the State. In the certifications required to be filed with their plans, the States will have to explain why this is not now technically possible and what steps are being taken to provide the technical capability by December 31, 1977. 20.23

Other Criminal History Record Systems

As noted, the minimum requirements set out in the regulations concerning disposition reporting and pre-dissemination queries to insure currency are applicable to records stored in central State repositories. This is because the regulations are based upon the premise that every State should have such a central repository and complete criminal history records should be maintained there and nowhere else. However, in the event that criminal history records are maintained at other criminal justice agencies, they are clearly subject to the requirements of Section 524(b) of the Safe Streets Act and thus to the general requirement in the regulations that criminal history record information be kept complete and accurate. Thus, if criminal histories are maintained at criminal justice agencies other than central repositories, and are available for dissemination outside of the agency, they must include dispositions to the maximum extent feasible, at least including all dispositions occurring in the jurisdiction served by the system containing the criminal history information.

The State plan must include an intention to advise such agencies of the requirement to obtain dispositions and to make appropriate inquiries before disseminating records to be sure they are current. Model procedures should be developed by the State, for use by these other repositories. These procedures should be as complete as those required of central repositories, and should include designations of officials responsible for obtaining dispositions, designations of officials in other agencies responsible for reporting dispositions, formal agreements between agencies supporting such arrangements, some method of assuring enforcement of the procedures and sanctions for failure to comply.

These requirements should not be interpreted as justification for the maintenance of criminal history records at the local level. On the contrary, the approach of the regulations is to encourage every

Regulations Reference

State to maintain such records at central State repositories and to discontinue to the maximum extent feasible the practice of maintaining criminal history records at local criminal justice agencies.

The regulations do not prohibit or impose controls on a system maintained by an agency for internal purposes, such as police investigative systems, as long as data contained therein is not disseminated outside the agency.

LIMITS ON DISSEMINATION

Dissemination means transmission of criminal history record information to individuals and agencies other than the criminal justice agency which maintains the criminal history record information. Dissemination includes confirmation of the existence or non-existence of a criminal history record. 20.21(b)

The plan must set forth operational procedures to limit dissemination of criminal history record information to the following individuals and agencies:

> "Criminal Justice Agencies where the information is to be used for administration of criminal justice purposes and criminal justice agency employment." [See definition of "criminal justice agency" in the instruction related to the commentary concerning 20.3(c)]. 20.21(b)(1)

> "Other individuals and agencies which require criminal history record information to implement a statute or executive order that expressly refers to criminal conduct and contains requirements and/or exclusions expressly based upon such conduct." 20.21(b)(2)

This exception is intended to permit public or private agencies to have access to criminal history record information where a statute or executive order:

- Denies employment, licensing, or other civil rights and privileges to persons convicted of a crime;
- Requires a criminal record check prior to employment, licensing, etc.

The above examples represent statutory patterns contemplated in drafting the regulations. The essential prerequisite for dissemination under this subsection is statutory reference to criminal conduct. Statutes which contain requirements and/or exclusions based on "good moral character" or "trustworthiness" would not be sufficient to authorize dissemination.

In the certification statement required by Section 20.22 to be submitted with each plan, the State is required to set forth a list of all non-criminal justice disseminations falling under this section of the regulations authorized by statutes or executive orders in effect at the time of plan submission, together with a description of the authorized non-criminal justice recipients and the purposes for which the information may be used. The States may conveniently use this listing as a starting point for a careful review of the general subject of non-criminal justice uses of criminal records in the State. It is strongly recommended that this be done and that careful consideration be given by each State to the enactment of comprehensive legislation on this subject, setting forth the purposes for which such disseminations may be permitted, the kinds of information that may be disseminated for particular purposes and the uses that may be made of the information.

It should be noted that the limitations on dissemination do not have to be fully implemented until December 31, 1977. Agencies, therefore, are not required to cease current dissemination practices. The delay in implementation was designed to give the States time to consider this matter and complete legislative action needed to comply with the regulations.

20.23

The language of the subsection will accommodate Civil Service suitability investigations under Executive Order 10450, which is the authority for most investigations conducted by the Commission. Section 3(a) of 10450 prescribes the minimum scope of investigation and requires a check of FBI fingerprint files and of written inquiries to appropriate law enforcement agencies.

> "Individuals and agencies pursuant to a specific agreement with a criminal justice agency to provide services required for the administration of criminal justice pursuant to that agreement. The agreement shall

> "specifically authorize access to data, limit the use of data to purposes for which given, insure the security and confidentiality of the data consistent with these regulations, and provide sanctions for violation thereof."

This subsection would permit private agencies such as the Vera Institute to receive criminal histories where they perform a necessary administration of justice function such as pretrial release. Private consulting firms which commonly assist criminal justice agencies in information systems development would also be included here.

> "Individuals and agencies for the express purpose of research, evaluative, or statistical activities pursuant to an agreement with a criminal justice agency. The agreement shall specifically authorize access to data, limit the use of data to research, evaluative, or statistical purposes, insure the confidentiality and security of the data consistent with these regulations and with Section 524(a) of the Act and any regulations implementing Section 524(a), and provide sanctions for the violation thereof."

Under this exception, any good faith researchers including private individuals would be permitted to use criminal history record information for reseach purposes. As with the agencies designated in 20.21(b)(3), researchers would be bound by an agreement with the disseminating criminal justice agency and would, of course, be subject to the sanctions of the Act.

The drafters of the regulations expressly rejected a suggestion which would have limited access for research purposes to certified research organizations. Specifically "certification" criteria would have been extremely difficult to draft and would have inevitably led to unnecessary restrictions on legitimate research.

Section 524(a) of the Act which forms part of the requirements of this section states:

> "Except as provided by Federal law other than this title, no officer

Regulations Reference

"or employee of the Federal Government, nor any recipient of assistance under the provisions of this title shall use or reveal any research or statistical information furnished under this title by any person and identifiable to any specific private person for any purpose other than the purpose for which it was obtained in accordance with this title. Copies of such information shall be immune from legal process, and shall not, without the consent of the person furnishing such information, be admitted as evidence or used for any purpose in any action, suit, or other judicial or administrative proceedings."

LEAA anticipates issuing regulations pursuant to Section 524(a) in the near future.

"Agencies of State or federal government which are authorized by statute or executive order to conduct investigations determining employment suitability or eligibility for security clearances allowing access to classified information." — 20.21(b)(5)

Dissemination under this exception would be permitted not only in cases of investigations of employment suitability, but also investigations relating to clearance of individuals for access to information which is classified pursuant to Executive Order 11652.

This exception, however, does not authorize dissemination where a statute or executive order authorizes an agency to conduct investigations for professional licensing such as barber, optometrist, etc. Agencies seeking dissemination of criminal history record information for licensing purposes must rely on the exceptions discussed pursuant to 20.21(b)(2).

"Individuals and agencies where authorized by court order or court rule." — 20.21(b)(6)

It is a general practice in many jurisdictions to give criminal history record information to bail bondsmen for the purpose of providing bail. In some States, bondsmen may be able to get criminal history record information pursuant to a specific statute or

Regulations Reference

agreement as provided in Subsection 20.21(b)(2) and (3). Where access pursuant to statute or agreement is not possible, it may be necessary for courts to promulgate a court rule permitting access to the information by bondsmen.

Confirming the existence or non-existence of criminal history record information is prohibited except relative to criminal justice agency employment, or other employment authorized by statute or executive order (including security clearance for employment). — 20.21(c)(3)

Dissemination of juvenile court records to non-criminal justice agencies is prohibited except where the dissemination takes place pursuant to (1) a statute or Federal executive order specifically authorizing juvenile record dissemination, (2) a good faith research agreement or (3) a contract to provide criminal justice service to the disseminating agency, or (4) a court order. Perhaps the most controversial part of this subsection is that it denies access to records of juveniles by federal non-criminal justice agencies conducting background investigations for eligibility to classified information under existing legal authority. — 20.21(d)

The above discussion on dissemination sets the outer limits of dissemination. Agencies having stricter dissemination and purging requirements are, of course, permitted to enforce such requirements. Neither these instructions nor the regulations mandate dissemination.

At a minimum, the following operable procedures must be included in the plan to insure that the dissemination restrictions of the preceding section are not violated.

Notice

It is likely that criminal history record information will be disseminated to agencies not directly subject to the regulations. Such agencies must be made aware of the provisions of these regulations aimed at preventing unauthorized disclosure.

Therefore, written notice to receiving agencies is an essential procedure to be detailed in the plan. Each disseminating agency subject to these regulations has the burden of giving notice of the requirement of the regulations.

Regulations Reference

The purpose of notice is to safeguard the privacy of individuals to whom the information relates. The notice, therefore, should specify restrictions on dissemination and internal agency use. It should also specify adequate security procedures consistent with the regulations. 20.21(c)(2)

Sanctions

The intent of the regulations will be undermined if receiving agencies not subject to the regulations are given criminal history record information with no controls. The plan, therefore, must provide sanctions which will subject non-federally funded agencies violating the regulations to equivalent or greater penalties than those applicable to federally funded agencies.

Sanctions against non-federally funded agencies may be applied by State legislation, contractual agreements, or other appropriate means.

If, for example, a State passes legislation specifying appropriate civil or criminal penalties for violation of the regulations by receiving agencies such legislation, if enforced in good faith, would meet the objective of the regulations.

An alternative procedure would be contractual agreements between disseminating and receiving agencies.

Accompanying the notice of the regulations would be a contractual agreement to which the receiving agency must expressly concur in writing. The agreement would specify that the dissemination of criminal history record information is subject to cancellation if the receiving agency knowingly violates the requirement relating to redissemination, internal use, and physical security.

The agreement would also stipulate that the receiving agency shall agree to be subject to fines under the regulation and the Act for knowingly violating the regulations.

Once notice of the regulations has been given and a receiving agency has agreed to abide by them, later disseminations to the receiving agency would be made under the same agreement.

The plan may provide for the development of a standard form contract by the State for use by all State and local agencies subject to these regulations.

Agencies disseminating criminal history record information to non-criminal justice government agencies, private agencies, and researchers would also make contractual arrangements similar to those required for criminal justice agencies. Such agreements would also provide that disseminated information and all copies thereof shall be returned to the disseminating agency or destroyed once the information is no longer needed for the purposes for which it was disseminated.

Validation

Before any dissemination takes place, disseminating agencies must be certain that the potential recipient is an agency permitted to receive information under the regulations.

If a potential non-criminal justice recipient claims to be authorized to receive information pursuant to a statute, executive order, or court order or rule, the disseminating agency must review the text of such authority prior to dissemination. If the disseminating agency is not certain that the rule, statute, or order is proper authority for dissemination, it should refuse to release the information pending an opinion by the LEAA Office of General Counsel.

Expiration of Availability

The regulations state that criminal history record information concerning the arrest of an individual may not be disseminated to a non-criminal justice agency or individual [except under Subsections 20.21(b)(3), (4), (5), (6)] if an interval of one year has elapsed from the date of the arrest and no disposition of the charge (by a prosecutor or court) has been recorded and no active prosecution of the charge is pending. (Where a person is a fugitive, prosecution is still active.) The arrest and disposition reporting process identified previously in these instructions should include the provisions for monitoring delinquent disposition information. If a delinquent disposition report monitoring system is not installed, provisions should be outlined in the plan to provide for restricting dissemination of delinquent disposition information at the time that discovery is made. 20.21(c)(1)

Computer terminal sites located in agencies authorized to receive such information should be notified via flags on the record or equivalent means

Regulations Reference

of notification that certain segments of the criminal history record are subject to restricted dissemination. This is to insure that computer terminal operators in remote sites will not mistakenly release restricted information to unauthorized sources.

Criminal history record information maintained on a manual basis should be visually screened to determine if restricted information is contained prior to the dissemination of the record to non-criminal justice agencies. Procedures should be established to appropriately identify record entries subject to the restrictions on dissemination.

Procedures should be presented in the plan which will provide specific guidance to clerical personnel retrieving and disseminating criminal history information. Additionally, procedures should be established for the update of the manual file to reflect data subject to restricted dissemination.

AUDITS AND QUALITY CONTROL

20.21(a)(2) and 20.21(e)

The regulations call for two different forms of auditing. The systematic audit is required for a repository as a means of guaranteeing the completeness and accuracy of the records. This audit is actually a quality control mechanism which should be part of the systems and procedures designed for a criminal history repository (either State or local). The annual audit is an examination, usually by an outside agency, of the extent to which any identified repository or user of such repositories are complying with the regulations.

Systematic Audit

This process refers to the combination of systems and procedures employed both to ensure completeness and to verify accuracy. Procedures dealing with checking on completeness, assuming the disposition reporting system described above, should provide a means for monitoring the submission of disposition data. Ideally, a State would institute a delinquent disposition monitoring system. Such a system would be based on estimating expected arrival dates for final dispositions, which reflect anticipated processing, for each type of criminal offense. If an expected disposition is not received by the estimated due date, the field staff then is automatically

Regulations Reference

notified and begins to make appropriate contacts and follow related audit trails to obtain the disposition information.

A requirement for delinquent disposition report monitoring applies to both manual and computerized systems. Procedures should be established in automated systems to automatically withhold the dissemination of information covered under the one-year rule to agencies maintaining terminal access to the system which are prohibited from receiving the information covered.

Accuracy checks require controls and inspections on the input to the system. In both manual and computerized systems, the auditing function would ensure that all record entries are verified and appropriately edited prior to entry, and that source documents are properly interpreted. Audit procedures should include random inspection of the records compared against source documents to determine if data-handling procedures are being correctly followed.

Audit Trail

An audit trail should be established which will allow for the tracing of specific data elements back to the source document. This audit trail should encompass all participating agencies in the criminal history records system and additionally should reflect specific individuals who have made entries on source documents or input formats supporting the system. It is imperative that provisions be made to provide a clear and specific audit trail for field staff personnel representing the central repository to insure that a maximum level of system accuracy is maintained.

Dissemination Logs

The audit trail covering input to the system must be followed by records of transactions in disseminating data in the system, so that accountability can be maintained over the full cycle of collection, storage, and dissemination of criminal history record information. Logging is required for the support of the audit process and also as a means of correcting erroneous dissemination.

The regulations state that criminal justice agencies "upon finding inaccurate information of a

20.21(a)(2)

material nature, shall notify all criminal justice agencies known to have received such information." The plan should identify procedures for maintaining a listing of the agencies or individuals both in and outside of the State to which criminal offender record information is released. This listing should be preserved for a period of not less than one year from the date of release. Such listings should indicate, as a minimum, the agency or individual to which information was released, the date of the release, the individual to whom the information relates, and the items of information released. The listings should include specific numeric or other unique identifiers to provide positive identification links between information which is disseminated and the record from which the information was extracted.

Procedures should be outlined in the plan to provide for immediately notifying agencies known to have received criminal history record information after inaccurate data has been entered on the record. Corrections to records should be forwarded immediately to all appropriate agencies in hardcopy forms such as letter or computer terminal printout. Procedures should be identified in the plan for recording the agencies to which corrections were sent and the date that the notifications were released.

Regulations Reference

20.21(e)

Annual Audit

The plan should set forth procedures that "insure that annual audits of a representative sample of State and local criminal justice agencies chosen on a random basis shall be conducted by the State to verify adherence to these regulations and that appropriate records shall be retained to facilitate such audits." Since the audit of each criminal justice agency would be cost prohibitive in most states, a "representative sample" is intended to provide a statistically significant examination of the accuracy and completeness of data maintained in a repository and to insure that the other provisions of the regulations are being upheld. Procedures must be identified in the plan providing for annual audits and outlining the specific sampling approach to be taken to include the number, type, location and size of agencies to be sampled (as expressed in population served). The authority to be held responsible to conduct the audit shall also be identified. It would be appropriate for the State central repository staff to conduct the audit of other State and local systems. Audit of the State central repository should be performed by another agency.

Regulations Reference

The annual audit should encompass all elements relative to the adherence of these regulations. Sampling procedures should be established for the examination of specific records at the repository level to be traced through internal update procedures back through field input processing to terminate at the source document. Areas to be reviewed should include, but not be limited to, record accuracy, completeness, review of the effectiveness of the systematic audit procedures, an examination of the evidence of dissemination limitations, security provisions, and the individual's right of access. The plan should address audits of both manual and computerized systems.

The plan should specifically identify documents and data elements to be maintained by local agencies necessary to support the annual audits. This documentation requirement should include, but not be limited to, maintaining source documents (at the point of data entry) from which criminal history information stored at the repository is derived.

Other information necessary to support annual audits are complete logs of dissemination maintained at each point authorized to release criminal history record data. These secondary logs should include as a minimum the names of all persons or agencies to whom information is disseminated as well as the date of release. The plan should identify any additional data elements to be contained in the dissemination logs which will appropriately complete the dissemination audit trail.

SECURITY

The regulations cover several aspects of security for criminal offender record information, including the hardware involved, personnel clearances, and facility security.

Dedicated Hardware

20.21(f)(2)

The regulations require that "where computerized data processing is employed, the hardware, including processor, communications control, and storage device to be utilized for the handling of criminal history record information is dedicated to purposes related to the administration of criminal justice."

To comply with the regulations, the hardware used to handle criminal history record information

must be "set aside" totally for the purpose of dealing with criminal justice data bases, criminal justice information exchange, or other purposes related to the administration of criminal justice.

The regulations specifically focus on the "hardware" employed in such a system. A computerized system contains many individual hardware components. It is possible to use a computerized system without using all of its hardware components. Therefore, the regulations do not necessarily require that the entire computer installation be set aside for criminal justice purposes. Specific hardware which would have to be used solely for criminal justice purposes would include the storage devices (such as disc, tape, or mass memory units of other kinds), terminals employed in accessing the criminal offender records, modems or other devices used to interface equipment with communications systems, the processor which has the function of controlling access to the records by receiving the inquiry and initiating any response to the inquiry, and any other processor used for updating files or otherwise handling the criminal history data.

The function of controlling access can be accomplished by a variety of hardware configurations. An increasingly common and acceptable approach is to use a separate computer more precisely engineered to handle the telecommunications function. These so-called "front-end" computers are physically distinct from any other processing unit which may be used, and they generally handle inquiry receipt and validation as well as response.

The use of a separate telecommunications processor provides a physical isolation of the portions of the system which provide access to the criminal offender records. The intent of the regulations is to ensure that access is controlled and to provide strict accountability for system operations. These purposes are easier to achieve with a system that has the physical isolation of a separate processor.

The plan should contain a thorough discussion of the approach to be taken to meet these requirements. The plan should present the general software and hardware procedures to be instituted to prohibit unauthorized access. These discussions should be directed toward all parts of the system identified by the State as the central repository for criminal offender record information.

Regulations Reference

For operational systems within the State other than the central repository, which are subject to these regulations, the State plan should include:

1. A survey of the extent to which these systems are using dedicated hardware.

2. Descriptions of the instructions which will be given to all users interfaced to the central repository computer system regarding the requirements for dedication.

Management Control — 20.21(f)(3)

To assure accountability for the operation of the system, a criminal justice agency is required to have the ability to set and enforce computer operations policy. To meet this requirement, the designated agency should be able to set priorities for user access, determine eligibility for direct access, apply sanctions for misuse of the system, select and dismiss staff, institute physical security measures, and perform other administrative functions normally associated with the management of operations.

Personnel Selection — 20.21(f)(5)

The regulations state that the plan shall set forth procedures which will "insure confidentiality and security of criminal history record information by providing that wherever criminal history record information is collected, stored, or disseminated, a criminal justice agency...shall select and supervise all personnel authorized to have direct access to such information." The plan should provide for a personnel clearance system for use in agencies which have the responsibility for maintaining or disseminating criminal history information. The plan should establish procedures for granting clearances for access to criminal history information as well as areas where criminal history data is maintained. These clearances should be granted in accordance with strict right-to-know and need-to-know principles. The personnel clearance system outlined in the plan should provide for selective clearances, allowing less than unconditional access to all areas. The clearance should be selective to the point of denying access because of the absence of the need to know. Clearances granted by one agency may be given full

Regulations Reference

faith and credit by another agency; however, ultimate responsibility for the integrity of the persons granted right-to-know clearances remains at all times with the agency granting the clearance.

Right-to-know clearances are executory and may be revoked or reduced to a lower sensitivity classification at the will of the grantor. Adequate notice must be given of the reduction or revocation to all other agencies that previously relied upon such clearances.

The plan should set forth specific training requirements for all personnel directly associated with the maintenance or dissemination of criminal history data. The training program should include the creation of a statewide training manual as well as training sessions to brief all personnel regarding the rules and regulations.

Physical Security — 20.21(f)(7)

The plan should not contain the details of security systems of individual agencies. The plan should indicate that procedures will be developed for the protection of information from environmental hazards including fire, flood, and power failure. Appropriate elements should include: (a) adequate fire detection and quenching systems; (b) watertight facilities; (c) protection against water and smoke damage; (d) liaison with local fire and public safety officials; (e) fire resistant materials of walls and floors; (f) air conditioning systems; (g) emergency power sources; and (h) backup files.

Agencies administering criminal justice information systems should adopt security procedures which limit physical access to information files. These procedures should include the use of guards, keys, badges, passwords, access restrictions, sign-in logs, or like controls. All facilities which house criminal justice information files should be so designed and constructed as to reduce the possibility of physical damage to the information. Appropriate steps in this regard include: physical limitations on access; security storage for information media; heavy-duty, non-exposed walls; perimeter barrier; adequate lighting; detection and warning devices; and closed circuit television. The plan should clearly outline these procedures or others which will accomplish an equivalent level of security for the physical facilities which contain criminal history information.

Regulations Reference

A record of transactions related to criminal history update information should be maintained on a computer-update log in automated systems or by a procedure which establishes an equivalent level of accountability. Manual systems accountability for record update information should be maintained on a manual log at the point of central record maintenance, or an equivalent method of accounting for criminal history record updates should be established.

INDIVIDUAL RIGHT OF ACCESS AND REVIEW — 20.21(g)

Each plan must provide for the institution of procedures to "insure the individual's right to access and review of criminal history information for purposes of accuracy and completeness." This procedure is required by the regulations to be "completely operational" upon plan submission. — 20.22(b)(1)

Although the regulations set out in some detail the essential elements that must be included in these procedures, maximum latitude is left to the States to devise procedures that best fit their systems.

The regulations provide that any individual "shall, upon satisfactory verification of his identity, be entitled to review, without undue burden to either the criminal justice agency or the individual, any criminal history record information maintained about the individual and obtain a copy thereof when necessary for the purpose of challenge or correction." Procedures to implement this provision should address the following issue at a minimum. — 20.21(g)(1)

Verification Method

The commentary on this subsection states that the drafters "expressly rejected a suggestion that would have called for a satisfactory verification of everyone's identity by fingerprint comparison." Thus, States are left free to use other methods of identity verification. For example, fingerprinting need not be required where the individual is well known to the official responsible for verification. This approach also leaves open the use of verification methods, such as voice print comparisons, that are now in the development stage but that may be available for routine use in the future. It should be stressed that States may elect to designate fingerprint comparisons as the required method of verification identity.

Regulations Reference

Rules for Access

Rules stating the procedures for access and review must be written and available to the public. The plan should state how these rules will be made publicly available, such as by publication in public journals, by distribution of pamphlets, by posters or by a combination of such methods.

The rules should cover such matters as the places where reviews may be had, the hours when reviews are available, any fees that are applicable, procedures for verification of identity, forms for making challenges, whether review must be in person or may be by counsel and rules for submitting explanatory material. The regulations do not deal with any of these matters, except to provide that the review may not involve "undue burden" to either the individual or the criminal justice agency. Thus, restrictions such as fees, location and hours should be reasonable and should not significantly restrict the individual's right to review his record.

In developing rules for access, States should have in mind the federal legislation on security and privacy of criminal justice information systems now pending in Congress. Both of the principal versions of the legislation now under consideration provide that an individual may review his record in person or through counsel. One version provides that fees must be "reasonable" and the other provides that fees may be charged "to the extent authorized by statute." States may wish to anticipate these requirements and provide for them even though the regulations do not include them.

Point of Review. The regulations provide that the individual's right to review applies to "any criminal history record information maintained about the individual." This means that some reasonably convenient method must be provided for review by the individual of criminal history information concerning him maintained anywhere in the State. The plan should specify where information will be available for review; that is, whether the individual must apply to a criminal justice agency where information about him is maintained or whether he may apply to any agency that can conveniently obtain the information for him. Although normally it will be permissible to require that the review take place at an agency that has custody or control of the record, this would, of course, not be permissible where complete records are

20.21(g)(1)

Regulations Reference

maintained only at a central repository located in another city. In such a case, the review should take place at a criminal justice agency convenient to the individual.

Obtaining a Copy. The procedures should specify the conditions under which a copy of an individual's record will be provided to him. Such copy should be prominently marked or stamped to indicate that the copy is for review and challenge only and that any other use thereof would be a violation of 42USC, page 3771. The commentary to this subsection of the regulations states that "a copy of the record should ordinarily only be given when it is clearly established that it is necessary for the purpose of challenge." This means that the individual bears the burden of showing his need for the copy. However, here again, it may be advisable to anticipate the requirements of the federal legislation and make copies available upon request. As a minimum, the individual should be given a copy of his record if after review he actually initiates a challenge and indicates that he needs the copy to pursue the challenge, unless because of the nature of the challenge it is clear that a copy is not necessary. The fee charged for providing the copy should not exceed actual costs of making the copy (including labor and materials cost). Typical fees now being charged for this service are in the $5 to $10 range.

20.21(g)(1)

Content of Challenge. The commentary to the regulations states that a "challenge" is "an oral or written contention by an individual that his record is inaccurate or incomplete." The commentary also provides that, as a part of a challenge procedure, the individual would be required "to give a correct version of his record and explain why he believes his version to be correct."

The plan should include procedures for making and recording challenges. These procedures may provide, for example, that all challenges shall be recorded on standard forms showing the name of the subject, the date and any exceptions taken or explanatory material offered. The individual may be required to fill in the form himself unless he cannot do so. He may be required to swear to the truth and accuracy of statements he makes in the challenge.

Administrative Review

20.21(g)(2)

The regulations state that the plan must provide for "administrative review and necessary correction

Regulations Reference

of any claim by the individual to whom the information relates that the information is inaccurate or incomplete." This requirement should be understood to mean that an individual who challenges his record is entitled to have the record appropriately corrected if there is no factual controversy concerning his challenge. If there is a factual controversy and it is resolved against him, he is entitled to a review of that decision by someone in the agency other than the person who made the decision.

The plan should specify time limits for the initial determination and for the determination after review. It should also require that published agency rules shall state the identity or titles of the individual or official with responsibility for administratively reviewing a decision not to correct a record.

Administrative Appeal — 20.21(g)(3)

The regulations provide that "the State shall establish and implement procedures for administrative appeal where a criminal justice agency refuses to correct challenged information to the satisfaction of the individual to whom the information relates." This should be understood to require a review by some impartial arbiter outside of the agency that made the determination not to correct the record to the individual's satisfaction. Provision for judicial appeal should not be construed as satisfying this requirement.

Designation of Appeal Body. The States are given great latitude to decide what group or body shall handle administrative appeals from challenges. They may utilize existing hearing procedures under State administrative procedure acts, a subunit of the State Attorney General's Office, or they may create a security and privacy council such as those that exist in several States.

Procedure for Appeal. The plan should state explicitly what steps an individual must take in order to obtain an appeal and applicable time limits. The plan should also set out in detail the procedures that will govern the appeal process.

This should include provisions as to whether the individual may be present, whether he may have counsel, whether he may present evidence and examine witnesses, whether a record of the proceedings will be kept, and how the decision of the appeal will be implemented.

Regulations Reference

Although the regulations leave these matters entirely to the discretion of the States, it should be borne in mind that both versions of the proposed federal legislation now pending in the Congress provide that the individual is entitled to a hearing at which he may appear with counsel, present evidence and examine and cross-examine witnesses.

Similarly, the possible impact of the federal legislation should be borne in mind by the States in deciding whether to make administrative decisions concerning challenges subject to judicial review. Although the regulations do not require that any means of judicial review be provided, both pending versions of the federal legislation do provide for civil actions to review final decisions of criminal justice agencies refusing to correct challenged information to the satisfaction of the individual. Thus, each State may wish to anticipate this requirement and provide in its plan for judicial review, if such review is not available under existing procedures for judicial review of final administrative actions by governmental agencies.

Correction Procedures — 20.21(g)(4)

The regulations provide that "upon request, an individual whose record has been corrected shall be given the name of all non-criminal justice agencies to whom the data has been given." This requirement enables the individual to take steps to correct erroneous information that may have been given to non-criminal justice agencies, since the regulations do not require that such agencies be notified of corrections by the correcting criminal justice agency. This requirement is, of course, directly related to the requirement in Section 20.21(e) of the regulations, which requires that records be kept of the names of all individuals or agencies to whom criminal history record information is disseminated. The plan should provide, either at this point or in the procedures implementing Section 20.21(e), for the maintenance of appropriate logs of non-criminal justice agency recipients. The plan should also set out procedures for preparing an appropriate list of such recipients, upon request of the individual, and making it available to him, including a designation of the agencies responsible for these steps. (The regulations do not require that the individual be given a list of non-criminal justice agencies or individuals to whom accurate and complete information has been disseminated.)

Regulations Reference

The regulations provide that "the correcting agency shall notify all criminal justice recipients of corrected information." This provision is related to the record-keeping provision of Section 20.21(e) and to the requirement set out in Section 20.21(a)(2) for notifying all criminal justice agencies known to have received information found to contain inaccuracies of a material nature. The plan must include procedures concerning the keeping of appropriate logs of disseminations to criminal justice agencies and fixing the responsibility for notifying those agencies that have received inaccurate information. Earlier in this section it was suggested that such logs should be maintained for one year. 20.21(g)(5)

Information Subject to Review

The individual's right to review under the regulations extends only to criminal history record information concerning him, as defined by Section 20.3(b) of the regulations. Hence, he is entitled to review information that records essentially the fact, date and results of each formal stage of the criminal justice process through which he passed to ensure that all such steps are completely and accurately recorded. He is not entitled under the regulations to review intelligence and investigative information. Nor is he entitled to review substantive information compiled about him by criminal justice agencies, as distinguished from a record of his movement through the agency. Thus, he would be entitled to review the recordation of his admission to bail, but not the bail report; the recordation of his sentencing, but not the presentence report; and the recordation of his admission to correctional institutions, but not medical records and other records of treatment.

If any of these reports are subject to dissemination, such as bail reports, parole reports or probation reports, and any correction is made in the individual's crminal history record as a result of a successful challenge, then appropriate corrections should of course be made in any of these reports that contain the erroneous information.

Regulations Reference

Section 3

CERTIFICATION STATEMENT

Each State must submit with its plan a certification stating the extent to which plan procedures have been implemented and detailing the steps undertaken to achieve full compliance. The evaluation by LEAA of the certification will be based upon "whether a good faith effort has been shown to initiate and/or further compliance with the plan and regulations." This section of the regulations also includes a requirement that all procedures in the approved plan must be fully operational and implemented by December 31, 1977--except for the computer hardware dedication requirement. LEAA may grant an extension of time upon a showing of "good cause." The certification also must include a listing of all existing statutory and executive order authority for non-criminal justice uses of criminal history record information in the State. 20.22 20.23 20.21(f)(2) 20.22(b)(5)

A certification consists of: 20.22(b)

(1) A checklist such as the sample enclosed for the central State repository.

(2) A checklist such as the sample enclosed for each other manual or automated system in the State covered by the regulations.

(3) A narrative discussion of problems impeding the implementation of the completeness and accuracy section of the regulations and what has been done about them.

(4) A listing of all relevant existing legislation authorizing dissemination to non-criminal justice agencies.

(5) A list (and summary description) of all enabling legislation or executive orders issued or pending that are related to complying with this legislation.

(6) The signature of the administrator of the agency designated by the Governor to submit the plan, attesting to the fact that the State has implemented the regulations to the maximum extent feasible.

Regulations Reference

The several separate components of the certification that are specifically required by the regulations are discussed below.

ACTIONS TAKEN AND DESCRIPTION OF SYSTEM CAPABILITY — 20.22(b)(1)

The certification must include "an outline of the action which has been instituted. At a minimum, the certification must state that the procedures for access and challenge by individual record subjects developed pursuant to Section 20.21(g) are completely operational."

The certification must also include a "description of existing system capability and steps being taken to upgrade such capability to meet the requirements of these regulations." — 20.22(b)(4)

States may satisfy the demands of the above two subsections by using a simple checklist. The checklist should briefly specify the principal operational procedures of the State plan, the applicable page references in the plan, and indicate by a simple yes or no whether the procedures have been implemented. (A sample checklist accompanies these instructions.)

It will obviously take time in some cases to obtain the authority, funds, personnel, and equipment necessary to implement State plans. The requirements acknowledge that a certification of compliance is not immediately necessary where implementation of a plan's procedures requires additional authority, involves unreasonable cost, or exceeds existing technical capability (included as technical capability are adequate personnel, equipment, and administrative arrangements). The above factors may, therefore, excuse non-implementation of the plan until December 31, 1977. After December 31, 1977, however, these plans must be totally operational throughout the State. — 20.22(a)

The checklist discussed above as an outline of action instituted may also be used to identify the reasons why portions of a plan have not been implemented. A portion of the checklist may thus be reserved to indicate if lack of legislative authority, funds, or technical capability is responsible for non-implementation. (See the sample checklist.)

EXAMPLE CERTIFICATION FOR A CENTRAL STATE REPOSITORY

Instructions Page Reference	OPERATIONAL PROCEDURES	Now Implemented	Reasons For Non-Implementation: Cost	Technical	Lack of Authority	Estimated Implementation Date
15	Completeness and Accuracy					
15	Central State Repository:					
16	Statutory/Executive Authority	___	___	___	___	___
16	Facilities and Staff	___	___	___	___	___
19	Complete Disposition Reporting in 90 days from:					
19	Police	___	___	___	___	___
19	Prosecutor	___	___	___	___	___
19	Trial Courts	___	___	___	___	___
19	Apellate Courts	___	___	___	___	___
19	Probation	___	___	___	___	___
19	Correctional Institutions	___	___	___	___	___
19	Parole	___	___	___	___	___
20	Query Before Dissemination:					
27	Notices/Agreements--Criminal Justice	___	___	___	___	___
30	Systematic Audit:					
31	Delinquent Disposition Monitoring	___	___	___	___	___
31	Accuracy Verification	___	___	___	___	___
31	Notice of Errors	___	___	___	___	___
23	Limits on Dissemination					
24	Contractual Agreements/Notices and Sanctions in Effect For:					
24	Criminal Justice Agencies	___	___	___	___	___
29	Non-Criminal Justice Agencies Granted Access by Law or Executive Order	___	___	___	___	___
24	Service Agencies Under Contract	___	___	___	___	___
29	Research Organizations	___	___	___	___	___
29	Validating Agency Right of Access	___	___	___	___	___
26	Restrictions On:					
27	Juvenile Record Dissemination	___	___	___	___	___
27	Confirmation of Record Existence	___	___	___	___	___
27	Secondary Dissemination by Non-Criminal Justice Agencies	___	___	___	___	___
29	Dissemination Without Disposition	___	___	___	___	___
30	Audits and Quality Control					
31	Audit Trail:					
31	Recreating Data Entry	___	___	___	___	___
31	Primary Dissemination Logs	___	___	___	___	___
31	Secondary Dissemination Logs	___	___	___	___	___
32	Annual Audit	___	___	___	___	___

EXAMPLE CERTIFICATION FOR A CENTRAL STATE REPOSITORY (Continued)

Instructions Page Reference	OPERATIONAL PROCEDURES	Now Implemented	Reasons For Non-Implementation: Cost	Technical	Lack of Authority	Estimated Implementation Date
	Security					
33	Executive/Statutory Designation of Responsible Criminal Justice Agency	___	___	___	___	___
34	Prevention of Unauthorized Access:					
34	Hardware Design	___	___	___	___	___
34	Software Design	___	___	___	___	___
33	Dedicated Hardware:					
34	Terminals	___	___	___	___	___
33	Communications Control	___	___	___	___	___
33	Processor	___	___	___	___	___
34	Storage Devices	___	___	___	___	___
35	Criminal Justice Agency Authority:					
35	Computer Operations Policy	___	___	___	___	___
35	Access to Work Areas	___	___	___	___	___
34	Selection and Supervision of Personnel	___	___	___	___	___
36	Assignment of Administrative Responsibility:					
36	Physical Security	___	___	___	___	___
36	Unauthorized Access	___	___	___	___	___
36	Physical Protection Against:					
36	Access to Equipment	___	___	___	___	___
36	Theft, Sabotage	___	___	___	___	___
36	Fire, Flood, Other Natural Disaster	___	___	___	___	___
36	Employee Training Program	___	___	___	___	___
37	Individual Right of Access					
38	Rules for Access	___				
38	Point of Review and Mechanism	___				
39	Challenge by Individual	___				
39	Administrative Review	___				
40	Administrative Appeal	___				
41	Correction/Notification of Error	___				

I certify that to the maximum extent feasible action has been taken to comply with the procedures set forth in the Privacy and Security Plan of the State of _____.

Signed _____

[Head of State Agency designated to be responsible for these regulations.]

EXAMPLE CERTIFICATION FOR AGENCY SYSTEMS OTHER THAN THE CENTRAL STATE REPOSITORY

Instructions Page Reference	OPERATIONAL PROCEDURES	Now Implemented	Reasons For Non-Implementation: Cost	Technical	Lack of Authority	Estimated Implementation Date
15	Completeness and Accuracy					
15	Central State Repository:					
16	Statutory/Executive Authority	___	___	___	___	___
16	Facilities and Staff	___	___	___	___	___
19	Complete Disposition Reporting in 90 days from:					
19	Police	___	___	___	___	___
19	Prosecutor	___	___	___	___	___
19	Trial Courts	___	___	___	___	___
19	Apellate Courts	___	___	___	___	___
19	Probation	___	___	___	___	___
19	Correctional Institutions	___	___	___	___	___
19	Parole	___	___	___	___	___
20	Query Before Dissemination:					
27	Notices/Agreements--Criminal Justice	___	___	___	___	___
30	Systematic Audit:					
31	Delinquent Disposition Monitoring	___	___	___	___	___
31	Accuracy Verification	___	___	___	___	___
31	Notice of Errors	___	___	___	___	___
23	Limits on Dissemination					
24	Contractual Agreements/Notices and Sanctions in Effect For:					
24	Criminal Justice Agencies	___	___	___	___	___
29	Non-Criminal Justice Agencies Granted Access by Law or Executive Order	___	___	___	___	___
24	Service Agencies Under Contract	___	___	___	___	___
29	Research Organizations	___	___	___	___	___
29	Validating Agency Right of Access	___	___	___	___	___
26	Restrictions On:					
27	Juvenile Record Dissemination	___	___	___	___	___
27	Confirmation of Record Existence	___	___	___	___	___
27	Secondary Dissemination by Non-Criminal Justice Agencies	___	___	___	___	___
29	Dissemination Without Disposition	___	___	___	___	___
30	Audits and Quality Control					
31	Audit Trail:					
31	Recreating Data Entry	___	___	___	___	___
31	Primary Dissemination Logs	___	___	___	___	___
31	Secondary Dissemination Logs	___	___	___	___	___
32	Annual Audit	___	___	___	___	___

EXAMPLE CERTIFICATION FOR AGENCY SYSTEMS OTHER THAN THE CENTRAL STATE REPOSITORY (Continued)

Instructions Page Reference	OPERATIONAL PROCEDURES	Now Implemented	Reasons For Non-Implementation: Cost	Technical	Lack of Authority	Estimated Implementation Date
	Security					
33	Executive/Statutory Designation of Responsible Criminal Justice Agency	___	___	___	___	___
34	Prevention of Unauthorized Access:					
34	Hardware Design	___	___	___	___	___
34	Software Design	___	___	___	___	___
33	Dedicated Hardware:					
34	Terminals	___	___	___	___	___
33	Communications Control	___	___	___	___	___
33	Processor	___	___	___	___	___
34	Storage Devices	___	___	___	___	___
35	Criminal Justice Agency Authority:					
35	Computer Operations Policy	___	___	___	___	___
35	Access to Work Areas	___	___	___	___	___
34	Selection and Supervision of Personnel	___	___	___	___	___
36	Assignment of Administrative Responsibility:					
36	Physical Security	___	___	___	___	___
36	Unauthorized Access	___	___	___	___	___
36	Physical Protection Against:					
36	Access to Equipment	___	___	___	___	___
36	Theft, Sabotage	___	___	___	___	___
36	Fire, Flood, Other Natural Disaster	___	___	___	___	___
36	Employee Training Program	___	___	___	___	___
37	Individual Right of Access					
38	Rules for Access	___				
38	Point of Review and Mechanism	___				
39	Challenge by Individual	___				
39	Administrative Review	___				
40	Administrative Appeal	___				
41	Correction/Notification of Error	___				

Regulations Reference

AUTHORIZING ORDERS AND LEGISLATION

20.22(b)(2)

The certification requires a "description of any legislation or executive order, or attempts to obtain such authority, that has been instituted to comply with these regulations." This should be understood to be partially covered in the previous section of the certification. If immediate compliance with certain plan procedures is impossible because of the lack of statutory or executive order authority, the certification must establish that steps have been taken to obtain such authority. Normally, necessary executive orders should have been issued by the Governor by the time of plan submission, unless they exceed his authority. Needed legislation should be in process to the maximum extent feasible under the circumstances, and the plan should identify the progress that has been made--drafted and introduced, undergoing hearings, awaiting the convening of a biennial legislative session, for example.

PROGRESS TOWARD PROBLEM RESOLUTION

20.22(b)(3)

The certification requires a description of "steps taken to overcome any fiscal, technical, and administrative barriers to the development of complete and accurate criminal history information." The demands of this subsection will be satisfied by a general discussion indicating what the State intends to do about disposition reporting and what the problems are.

Adequate disposition reporting is at the heart of the completeness and accuracy provision. States may satisfy the requirements of this subsection by a discussion of what the State intends to do to insure up-to-date disposition data and what the problems in implementation are. For example, if the plan contemplates the establishment of a central State repository to provide full criminal history storage and criminal identification services to all agencies throughout the State, and if the repository is not fully operational and able to respond to all user needs at the time of plan submission, certification should explain the extent to which implementation has been achieved and identify the factors--such as lack of trained personnel or funds for automated data processing equipment--that have prevented full implementation. Discussion under this subsection should not exceed five pages.

Regulations Reference
20.22(b)(5)

STATUTORY AUTHORITY FOR NON-CRIMINAL JUSTICE USES

The certification requires a "listing setting forth all non-criminal justice dissemination authorized by legislation existing as of the date of the certification showing the specific categories of non-criminal justice individuals or agencies, the specific purposes or uses for which information may be disseminated, and the statutory or executive order citations."

This section of the certification is directly related to Section 20.21(b)(2) which limits the dissemination and use of criminal records for non-criminal justice purposes to those instances where the information is required to implement a statute or executive order that contains requirements or exclusions expressly related to criminal conduct. This section is discussed earlier in these guidelines.

The certification must set forth a compilation of all statutes and executive orders in effect in the State that meet the requirements of Section 20.21(b)(2), together with citations. The compilation should set out for each such statute or executive order the prevailing interpretation in the State as to what agencies and individuals are authorized to receive criminal record information under its authority and the specific purposes or uses authorized.

Regulations Reference

Section 4

PENALTIES FOR NON-COMPLIANCE WITH THE REGULATIONS 20.25

Agencies may be subject to the penalties of the Act for knowing and willful failure to comply with any of the following requirements:

(1) failure to submit an adequate plan,

(2) failure to submit adequate certification and,

(3) failure to comply with the specific requirements of the regulations, including failure to implement operational procedures set forth in the plan by December 31, 1977.

A good faith misinterpretation or lack of knowledge by an agency or individual of the regulations or operational procedures set forth in the State plan may excuse failure to comply.

FAILURE TO SUBMIT ADEQUATE PLAN OR CERTIFICATIONS

Submission of certification and a plan are the responsibility of the agency designated by the Governor of the State. A maximum of 90 days' extension will be permitted in the case of inadequate plans or certifications. The extension period could, however, be less than 90 days, if in the judgment of LEAA the deficiencies can be corrected in a shorter period of time.

Failure to provide an adequate plan or certification may subject the State to partial or total fund cutoffs by LEAA and to the imposition of a $10,000 fine.

FAILURE TO COMPLY WITH SPECIFIC PROVISIONS

The Effect of Certification 20.23

The regulations provide for subsequent annual certifications of action taken by the State, if compliance with the regulations is not complete at the time of the initial certification. LEAA recognizes that criminal justice agencies and other agencies

will probably not be able to comply immediately with all of the requirements of the regulations. Most States may find it is necessary, therefore, to submit more than one annual certification.

Once a State states in its certification that the action necessary to implement a specific portion of the regulations is completed, willful and knowing non-compliance by State or local agencies with the regulations could subject the agency involved to the fines and cutoff penalties provided in the regulations and Act.

Non-Compliance After 1977 Deadline — 20.23

In addition, all procedures in a plan must be fully operational and implemented by December 31, 1977. The knowing and willful failure by any State or local agency to comply with the plan's procedures after that date will subject the agency to the sanctions under the regulations and Act. The only exception to the 1977 deadline is the requirement of dedication of computer configurations in 20.21(f)(2). State and local agencies may be allowed additional periods of time to implement the dedication requirement upon the submission of a written application to LEAA stating good cause for the extension of the deadline. The fact that the dedication requirement would cause highly excessive increases in present criminal justice systems expenditures consitutes good cause. Adequate data must be provided to justify any extension beyond the December 31, 1977 deadline for compliance. Where it appears that an extension is warranted, States should submit plans, where possible, for reconfiguration of existing hardware in order that dedication can be achieved. Where such reconfiguration is not possible States should submit a brief description of alternative means of compliance in order to provide adequate security protection of criminal history record information.

ACKNOWLEDGEMENTS

The foregoing materials were prepared under the auspices of Public Systems inc. The authors of this report are:

Dan George
Lawrence Leigh
Michael Stewart
Paul Woodard
Paul Wormeli

The authors wish to acknowledge the direct and valuable contributions made in reviewing this document by:

(1) SEARCH Group, Incorporated, its staff, the Standing Committees on Security and Privacy and Legislative Review

(2) The staff of the National Governor's Conference;

(3) LEAA staff, including Mr. Thomas Madden (LEAA General Counsel), Mr. Harry Bratt (Acting Director of the National Criminal Justice Information and Statistics Service), Ms. Helen Lessen (Office of General Counsel) and Ms. Carol Kaplan who is the LEAA Project Director for this effort.

Paul K. Wormeli
Vice President
Public Systems inc.

PRIVACY AND SECURITY
PLANNING INSTRUCTIONS

Supplement No. 1

August 20, 1975

Law Enforcement Assistance Administration
U. S. Department of Justice

These supplemental instructions are being distributed in response to questions raised since the issuance of the LEAA Privacy and Security Planning Instructions dated June 30, 1975. The supplement deals with material in the initial instructions that appears to require more clarification, in view of the questions directed to LEAA.

The supplemental instructions should only be read in conjunction with the regulations and with the basic instructions.

APPLICABILITY

The regulations were written with the intent of covering collections of records containing historical references to a person's involvement with criminal justice agencies. Such a collection of records would have (potentially) a listing of more than one event, such as a listing of all arrests. This file would also be accessible by the name of the person, so that an inquiry by name could produce a listing of many or all actions taken relating to the subject by criminal justice agencies.

To ensure that all instances are covered under which such a collection of records was maintained, the regulations and the commentary create two tests to determine whether or not any particular collection of records is criminal history record information. Essentially, to qualify for inclusion in the definition, the individual records so assembled must contain both (1) identification data sufficient to identify the subject of the record and (2) notations regarding any "formal criminal justice transaction" involving the identified individual. To be more precise, the types of transactions referred to are those defined by the OBTS/CCH data base designs.

Many files or systems maintained by local agencies qualify for inclusion under this definition. For example, the regulations would apply to criminal history information contained in police files indicating for each person therein notations of the arrests of the person, prosecutor files or systems indicating the convictions or arrests relating to an individual, accumulations of presentence reports or probation reports containing information on prior criminal involvement, and so on.

It was not intended that the definition apply to the document originally prepared to record the facts about the transaction. Such original records of entry would include the report of a crime scene investigation (filled out by the investigating officer), each individual arrest report describing the arrest and circumstances surrounding the arrest, the report of court action on an individual, etc. These original documents are specifically exempted from the applicability of the regulations, except as discussed below.

When an agency brings together all of these source documents pertaining to an individual, this collection of records may become criminal history record information. The collected documents (records) in this circumstance continue to be excluded from the definition and from coverage by the regulations only if they are organized and accessed chronologically. That is, if these original documents are filed alphabetically,

thereby allowing a search by name for retrieval of all such records related to a single person, the collection of records then falls under the definition of criminal history record information. Likewise, any index to these documents that permits a search of the collection on the basis of name would, in conjunction with the documents, be criminal history record information.

Even though a collection of records qualifies under the definition, the extent to which the regulations apply may vary depending on what is done with the records, and therefore the impact of the regulations on the agency may vary. The accompanying chart indicates the factors which affect the impact of the regulations and the consequent procedures required. For example, agencies which are covered by the regulations but do not disseminate CHRI (Column 9 or 11) need not comply with the restrictions on completeness.

It is not possible to avoid the regulations by separating parts of a file or data system. Under the regulations, the physical distribution of the records is not relevant. As long as the name access is permitted, and the access method effectively links the records together in retrieving them, the system falls under the definition.

Some misunderstanding was apparently generated by the statement on page 7 of the Privacy and Security Planning Instructions which limited criminal history record information only to offenses where fingerprints were taken. This interpretation was made to support the development of complete and accurate records, inasmuch as the verification of identity by fingerprints should be a fundamental rule governing the entry of data into a criminal history file. The language of the instructions, unfortunately, gives the impression that coverage under the regulations could be avoided by not taking fingerprints at any point. Thus, such unsupported records could be freely disseminated.

This understanding of the instructions is incorrect. Fingerprints do not have to be taken to cause a record to be criminal history record information. If such a record [as defined in 20.3(b)] is started, then all parts of the regulations would apply to these records, including the requirement to obtain dispositions and to ensure the accuracy of the record.

It should be noted that the completeness and accuracy requirement would apply to any criminal history record information available for dissemination, not just the information in a State central repository.

Section 20.20(c) uses the phase "reasonably contemporaneous" to relate to public disclosure of criminal justice transactions. This phrase is intended to mean a time period during which a

APPLICABILITY AND IMPACT OF REGULATIONS

Find the column that characterizes your agency in terms of the four applicability criteria, then read down the column to find the impact of the regulations.

	Possible Combinations of Applicability Criteria												
APPLICABILITY CRITERIA:	1	2	3	4	5	6	7	8	9	10	11	12	13
Received LEAA Funds for CHRI	No	No	No	No	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes
Collects/ Maintains CHRI	No	Yes	Yes	No	Yes	Yes	No	No	Yes	No	Yes	Yes	Yes
Disseminates CHRI	No	No	Yes	No	No	Yes	Yes	No	No	Yes	No	Yes	Yes
Receives CHRI	No	No	No	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	No	Yes
	Totally Unaffected By Regulations			Required to Comply Only As Specified in CHRI Use Agreements									
OPERATIONAL PROCEDURES REQUIRED:													
Required to submit certification	X	X	X	X	X								
Completeness (Disposition Reporting)				X	X								
Query before dissemination		X		X	X								
Accuracy--quality control and audit	X		X	X	X								
Prepare procedures/agreements limiting dissemination		X		X	X								
Maintain dissemination logs		X		X	X								
Technical provisions limiting access	X	X	X	X	X								
Dedicated hardware	X	X	X	X	X								
Control of computer operations	X	X	X	X	X								
Physical security/protection	X	X	X	X	X								
Individual right of access	X		X	X	X								

particular transaction would be current news. This would include, for example, disclosure during or before trial of arrest information regarding the offense which is or is to be the subject of the trial.

DISSEMINATION

The regulations do not precisely define dissemination. However, it can be interpreted to apply to the release of criminal history record information by an agency to another agency or individual. Use of the information by an employee or officer of the agency maintaining the records does not constitute dissemination. Further, reporting the occurrence of and the circumstances of a criminal justice transaction is not dissemination. That is, the reporting of an arrest or other transaction to a local or State repository is not dissemination. Similarly, reporting data on a particular transaction to another criminal justice agency so as to permit the initiation of subsequent criminal justice proceedings is not considered to be dissemination (for example, police departments may deliver arrest reports to a prosecutor as part of the documentation required for prosecutorial action).

INDIVIDUAL'S RIGHT OF ACCESS

Dissemination to the subject of a record is permitted only for the purposes of challenge and correction. It is only necessary to deliver a hand copy of that portion of the record which is to be challenged.

Any attempt by employers to subvent the restrictions on dissemination by requiring prospective employees to obtain a copy of their criminal history can thus be discouraged by making it a practice only to give the subject a copy of that portion of the record which is to be challenged, and then only after the challenge process is actually initiated (such as by filing a claim of inaccuracy). Furthermore, the regulations do not require any written documentation to be given to an individual attesting to the lack of a record. Such a "good character" letter would be confirmation of the existence or non-existence of criminal history record information, is defined to be dissemination, and is therefore limited by the regulations to the purposes defined in Section 20.21(c)(3).

Confirmation to criminal justice agencies of the non-existence of a criminal history record does not require the maintenance of a dissemination log.

TRANSMISSION OF CRIMINAL HISTORY RECORD INFORMATION

The regulations are silent on the direct questions of controlling transmission of these records via various kinds of networks. However, the regulations do require that direct access to the records shall be limited to employees and officers of a criminal justice agency. Therefore, the use of any transmission medium which does not afford reasonable assurances that access is so controlled would be prohibited under the regulations.

Based on the present level of experience, it would appear that the probability of telephone line interception for the purpose of gaining access to criminal history information is so low as to permit the use of telephone lines for this purpose. Also, information transmitted in digital form, using standard telecommunications codes, would be sufficiently difficult to reconstruct so as to permit such transmission unless the transmitting agency has reason to doubt the security.

On the other hand, uncoded voice transmission over radio links are easily intercepted, and it is unlikely that such transmissions could be protected to the extent required.

The transmitting agency must also assume itself that the receiving site sustains a reasonable level of security.

PRIVACY AND SECURITY
PLANNING INSTRUCTIONS

Supplement No. 2

September 30, 1975

Law Enforcement Assistance Administration
U. S. Department of Justice

These supplemental instructions are being distributed in response to questions raised since the issuance of the LEAA Privacy and Security Planning Instructions dated June 30, 1975. The supplement deals with material in the initial instructions that appears to require more clarification, in view of the questions directed to LEAA.

These supplemental instructions should be read in conjunction with the regulations, the basic instructions, and with Supplement No. 1 issued August 20, 1975.

USER AGREEMENTS

The regulations (Section 20.21(b)) require each state plan to insure that dissemination of criminal history record information has been limited, "whether directly or through any intermediary," only to criminal justice agencies and specified categories of legally-authorized non-criminal justice agencies and individuals. Therefore, each state plan must set forth procedures to insure that criminal justice agencies will themselves comply with the limits on dissemination, and also that these limits will be observed by agencies and individuals to whom they disseminate records; that is, that secondary disseminations will conform to the regulations.

In effect, this means that, whenever a criminal justice agency subject to the regulations receives a request for a record, it must, before dissemination, determine that the requesting agency or individual is (1) an eligible recipient and (2) aware of and subject to the limits on use and dissemination imposed by the regulations. In addition to the limits set by Section 20.21(b), non-criminal justice recipients must be aware of and subject to the provisions of Section 20.21(c) (2) prohibiting secondary disseminations and restricting the use of criminal history records to the specific purposes for which they were made available. All recipients must agree to enforce appropriate measures to insure the security and confidentiality of criminal history records.

Criminal justice agencies that have received LEAA funds for support of criminal history record systems since July 1, 1973, are directly covered by the regulations and will be required to submit certifications attesting to their awareness of the regulations and to the existence of procedures designed to insure compliance with all provisions of the regulations. However, criminal justice agencies that have not received LEAA funds for system support since July 1, 1973, are not subject to the regulations and are not required to submit certifications. In addition, none of the numerous non-criminal justice organizations and individuals that may be eligible to receive criminal history records under categories (2) through (6) of Section 20.21(b) would be directly covered by the regulations. Each state plan must set forth some means of insuring that the regulations, or equivalent limits and requirements, can be made applicable to these agencies and individuals.

By far the preferable means of accomplishing this would be the enactment of a comprehensive state statute covering all such record users and imposing upon them requirements and limits at least as stringent as those set out in the regulations, with sanctions and penalties for violations. Any

non-certified agency or individual not covered by such a statute must be required to enter into a written user agreement with a certified criminal justice agency.

In summary, in order to receive criminal history records, agencies and individuals must be determined to be both eligible under Section 20.21(b) and subject to the regulations by virtue of a certification, a state statute or a user agreement.

User agreements should specify the basis of eligibility under Section 20.21(b) and the specific purposes for which the released records may be used, and should contain an acknowledgement by the recipient agency or individual that the records are subject to limits on use and redissemination set out in the regulations and that violation of these limits will result in the imposition of penalties and sanctions. The agreements should expressly state that the user agency or individual agrees to be bound by the terms of the regulations on a continuing basis with respect to any criminal history record information received from any agency within or outside of the state. In developing the form of these agreements, states may wish to refer to Project SEARCH Technical Memorandum No. 5, published in November, 1973, entitled "Terminal Users Agreement for CCH and Other Criminal Justice Information."

It is not required that each criminal justice agency obtain a certification or execute a user agreement with every agency or individual to whom it disseminates information, if each such agency or individual has submitted a certification to the state or has signed a user agreement with some other criminal justice agency. Normally all such agreements should be executed with the central state repository or some other designated central agency. In the absence of such a central agency, the agreement should be signed with the criminal justice agency from which the user first obtains criminal history record information. Criminal justice agencies may accept oral representations that requesting agencies, either in or out of the state, have submitted certifications or have signed user agreements incorporating the limits and requirements of the regulations.

SECURITY

The use of non-criminal justice personnel (such as individuals from other government agencies or contractor services) is permissible under the regulations for purposes of system development, including programming and data conversion. Access to criminal history data by these individuals is authorized by Section 20.21(b) (3), but only to the extent "required for the administration of criminal justice." Access must be granted by

means of an agreement or contract which specifies limitations on use and provides sanctions for the breach of security procedures.

When such personnel are utilized, they are under the direction of and performing duties for the benefit of a criminal justice agency. It would be reasonable to consider such individuals, for the purposes of the security section of the regulations, to be equivalent to employees of a criminal justice agency. Therefore, the same security procedures could be applied. In practice, this approach would mean that where a person has unlimited access to the data base, the same level of personnel clearance should be obtained as would be sought for a full-time criminal justice agency employee in similar situations.

It is not mandatory that all persons having physical access to a data center be required to have a security clearance. Procedures such as use of escorts, equipment access limitations, etc., can be used where appropriate.

RECORD SYSTEMS COVERED

To clarify the specific kinds of record systems which may be covered by the regulations, Exhibit 1 shows the extent of coverage for some typical systems. It should be noted that the procedures required in the event a particular file qualifies for inclusion will vary, depending primarily on the extent of dissemination.

COURT RECORDS

Section 20.20(b)(3) provides that the regulations do not apply to criminal history record information contained in: "court records of public judicial proceedings compiled chronologically" means that the various parts of a record are arranged (as a general rule) according to an ordered time sequence, and results from criminal charges filed in a single case.

The purpose of this exception is to permit access to records which traditionally have been open to the public, defendants, or members of the bar. The basic model contemplated by the drafters is the register of cases maintained in most county clerk's offices. Entries are made in the registers as cases arise, and the outcomes of various motions, conferences, leavings and other stages of the adjudication are filed as they occur. Also included under this exception would be individual case files containing the trial transcript and

Exhibit 1. EXAMPLES OF THE EXTENT OF
COVERAGE OF THE PRIVACY AND SECURITY REGULATIONS

Type of Record System	Features	Coverage
Subject-in-process	Intra-jurisdictional scope, multiple agency input, storage, multi-agency access	Yes
		No, if arrestee not indicated
Crime incident file	Time, place characteristics of event	No, unless also used to record detention/ arrests
Field interview file	Citizen interview by police officer	Yes
		No, (only any CHRI contained therein)
Local Ordinance violations	Arrests/detentions for vagrancy, traffic, disorderly conduct, etc.	No
Intelligence files	Investigative observations, associations	Yes
Court case file	State vs. _____, filed chronologically or by number derived chronologically	Yes, (need not be complete if only used internally)
Alphabetical indexes to court or police case files	Name vs. case number	No
M.O. files	Data on all persons arrested/ convicted for a particular offense	
Court calendaring	Scheduled dates of actions, names of participants (excluding references to arrests or dispositions)	

other records accumulated in the course of the case. One important caveat, however, must be issued. "Rap sheets" or summary criminal histories are sometimes included in such files, as a matter of administrative practice in filing. These documents are not considered "court records" under this section and are not exempt from coverage under the regulations.

Alphabetical indexes to court records are generally not exempt. For example, an alphabetical index to case files such as the following would be subject to the regulations:

Name	Case Action Number
John Jay	#75051
John Jensen	#59607 #65030 #76031
John Johnson	#59603 #58601

The regulations apply to combinations of any non-chronological index and file which might be used to assemble or permit retrieval of a summary criminal history on an individual. If as a result of automatic data processing, the equivalent to an alphabetical manual index exists, such automated files would likewise be subject to the regulations.

On page 8 of the original Privacy and Security Planning Instructions the discussion of the "court records" exception may suggest a broader interpretation of the exception than has been indicated above. To the extent that it does so, the discussion should be disregarded.

LEGISLATIVE PROGRAM TO COMPLY WITH REGULATIONS

The following items may be done by Executive Order; but, in all cases, a statute would be preferable.

1. Statutory authority for criminal justice agencies (or Executive Order).
2. Mandatory disposition reporting law.
3. Establishment of Central State Repository.

4. Comprehensive legislation on non-criminal justice uses.

5. Statutory basis for certain agencies to have access to criminal records and juvenile delinquency records:

   Public Defender Offices
   Private defense attorneys
   Bail bondsmen
   State Civil Service Commissions
   Others

6. Establishment of Criminal History Control Board.

7. Right of individual to review and challenge--expanding on regulations, providing judicial review, setting penalties.

8. Prohibition against private employers, etc., requiring an individual to turn over a copy of his record obtained for challenge.

9. Penalties, particularly applicable to agencies and individuals not covered by Section 524(b) including:

   Administrative sanctions
   Civil remedies
   Criminal penalties

ACCESS BY THE MILITARY

LEAA has ruled that Section 20.21(b)(2) of the regulations permits dissemination of adult criminal history record information to military recruiters, unless otherwise prohibited by the state.

Section 20.21(b)(2) of the regulations authorizes dissemination of criminal history record information to individuals or agencies if three criteria are met:

1. The information must be necessary for the implementation of a statute or executive order.

2. The statute must contain express references to criminal conduct.

3. The statute must contain requirements and/or exclusions expressly based upon such conduct.

This section is intended to allow access to criminal history record information by agencies in instances where a statute or executive order specifically denies employement,

licensing or other civil rights and privileges to persons convicted of a crime. Statutes which contain general requirements of "good moral character" or the like, are not sufficient to authorize dissemination.

10 U.S.C. Section 504 states that, except with special permission, no person who has been convicted of a felony may be enlisted in the armed forces. This statute fulfills the requirements of Section 20.21(b)(2). The information is required by military recruiters so that they may insure that only qualified persons are allowed to enlist; the statute specifically refers to felonious conduct; and the statute expressly provides that persons convicted of felonies will be excluded from the armed services. This is precisely the type of situation for which Section 20.21 was designed.

Section 20.21(d) prohibits dissemination of juvenile records except pursuant to a statute or Federal executive order which specifically refers to and permits dissemination of juvenile records. 10 U.S.C. Section 504, not containing any reference to juveniles, does not fulfill this requirement. In the absence of any other statute or Federal executive order conferring such authority, juvenile records may not be accessed.

CERTIFICATION

The original instructions (dated June 30) contained two suggested checklists which could be used as a basis for certification. The list suggested as an example for systems other than the central repository was erroneously copied from the list suggested for the central repository. The correct checklist is shown in Exhibit 2.

COURT RULES/ORDERS

Court rules or orders permitting class access should be limited to classes of recipients involved in the criminal justice process. This would include, e.g., (1) bail bondsmen (2) defense attorneys, and (3) private community corrections programs.

Court orders concerning non-criminal justice-related recipients should be strictly ad hoc--limited to instances where a particular individual or agency applies for access that is not otherwise permissible and is able to show extraordinary circumstances. An example in the commentary is that in "extraordinary circumstances" an individual might get a court order permitting a "no record" certification to take to an employer.

This approach means that a court could not issue a blanket court order or rule permitting all employers, or even certain types of employers, to have criminal records where there is no statute or executive order covering them.

In other words, a court order can grant specific "good cause" exceptions to the non-criminal justice dissemination limits, but cannot grant class or group exceptions that would have the effect of nullifying the limits under other categories of Section 20.21(b).

DISSEMINATION

The reporting of criminal history record information to the FBI is similar to reporting to a central state repository and does not constitute dissemination.

EXAMPLE CERTIFICATION FOR AGENCY SYSTEMS OTHER THAN THE CENTRAL STATE REPOSITORY

Instructions Page Reference	OPERATIONAL PROCEDURES	Now Implemented	Reasons For Non-Implementation: Cost	Technical	Lack of Authority	Estimated Implementation Date
	Completeness and Accuracy					
19	Complete Disposition Reporting from:					
19	Police	___	___	___	___	___
19	Prosecutor	___	___	___	___	___
19	Trial Courts	___	___	___	___	___
19	Appellate Courts	___	___	___	___	___
19	Probation	___	___	___	___	___
19	Correctional Institutions	___	___	___	___	___
19	Parole	___	___	___	___	___
20	Query Before Dissemination	___	___	___	___	___
30	Systematic Audit:					
31	Delinquent Disposition Monitoring	___	___	___	___	___
31	Accuracy verification	___	___	___	___	___
23	Limits on Dissemination					
24	Contractual Agreements/Notices and Sanctions in Effect For:					
24	Criminal Justice Agencies	___	___	___	___	___
29	Non-Criminal Justice Agencies Granted Access by Law or Executive Order	___	___	___	___	___
24	Service Agencies Under Contract	___	___	___	___	___
29	Research Organizations	___	___	___	___	___
29	Validating Agency Right of Access	___	___	___	___	___
26	Restrictions On:					
27	Juvenile Record Dissemination	___	___	___	___	___
27	Confirmation of Record Existence	___	___	___	___	___
27	Secondary Dissemination by Non-Criminal Justice Agencies	___	___	___	___	___
29	Dissemination Without Disposition	___	___	___	___	___
30	Audits and Quality Control					
31	Audit Trail:					
31	Recreating Data Entry	___	___	___	___	___
31	Primary Dissemination Logs	___	___	___	___	___
31	Secondary Dissemination Logs	___	___	___	___	___

EXAMPLE CERTIFICATION FOR AGENCY SYSTEMS
OTHER THAN THE CENTRAL STATE REPOSITORY
(Continued)

Instructions Page Reference	OPERATIONAL PROCEDURES	Now Implemented	Reasons For Non-Implementation			Estimated Implementation Date
			Cost	Technical	Lack of Authority	
	Security					
33	Executive/Statutory Designation of Responsible Criminal Justice Agency	___	___	___	___	___
34	Prevention of Unauthorized Access:					
34	Hardware Design	___	___	___	___	___
34	Software Design	___	___	___	___	___
33	Dedicated Hardware:					
34	Terminals	___	___	___	___	___
33	Communications Control	___	___	___	___	___
33	Processor	___	___	___	___	___
34	Storage Devices	___	___	___	___	___
35	Criminal Justice Agency Authority:					
35	Computer Operations Policy	___	___	___	___	___
35	Access to Work Areas	___	___	___	___	___
34	Selection and Supervision of Personnel	___	___	___	___	___
36	Assignment of Administrative Responsibility:					
36	Physical Security	___	___	___	___	___
36	Unauthorized Access	___	___	___	___	___
36	Physical Protection Against:					
36	Access to Equipment	___	___	___	___	___
36	Theft, Sabotage	___	___	___	___	___
36	Fire, Flood, Other Natural Disaster	___	___	___	___	___
36	Employee Training Program	___	___	___	___	___
37	Individual Right of Access					
38	Rules for Access	___				
38	Point of Review and Mechanism	___				
39	Challenge by Individual	___				
39	Administrative Review	___				
40	Administrative Appeal	___				
41	Correction/Notification of Error	___				

END