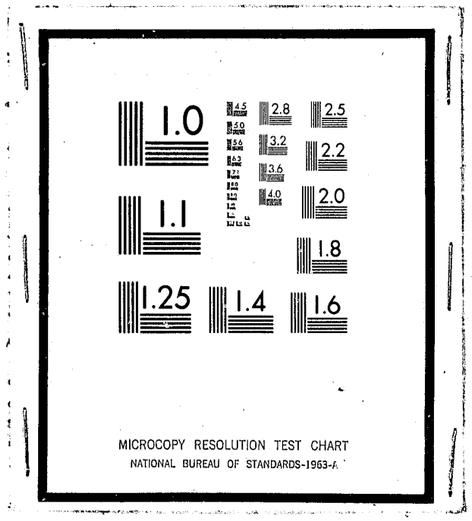

Privacy and Security Planning Instructions

CRIMINAL JUSTICE INFORMATION SYSTEMS

Revised
April 1976

U. S. DEPARTMENT OF JUSTICE
Law Enforcement Assistance Administration
National Criminal Justice Information and Statistics Service

Privacy and Security Planning Instructions

CRIMINAL JUSTICE INFORMATION SYSTEMS

Revised
April 1976

U. S. DEPARTMENT OF JUSTICE
Law Enforcement Assistance Administration
National Criminal Justice Information and Statistics Service

U.S. Department of Justice
Law Enforcement Assistance Administration
National Criminal Justice Information Statistics Service

Richard W. Velde
Administrator

Henry F. McQuade
Deputy Administrator for Policy Development

Paul K. Wormeli
Deputy Administrator for Administration

Harry Bratt
Assistant Administrator
National Criminal Justice Information and Statistics Service

Carol G. Kaplan, Director
Privacy and Security Staff

PREFACE

These instructions have been prepared to provide clarification and explanation of the Department of Justice regulations governing criminal justice information systems, as amended March 19, 1976. 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 and implementing 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 originally issued on June 30, 1975. They have been revised to accommodate the March 19, 1976 amendments to the regulations. This revised edition of the instructions also incorporates Supplements 1 and 2, as well as other changes resulting from questions raised during the privacy planning workshops in 1975. This is the final edition of the instructions. Any further questions of a substantive nature should be addressed to:

NCJISS
LEAA
Washington, D.C. 20531

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 called for each State to prepare a State plan and to submit the plan to LEAA for approval by December 16, 1975. By notice published in the Federal Register on October 24, 1975 (40 FR 49789), the plan submission date was changed to March 16, 1976. On March 19, 1976, amendments to the regulations were published in the Federal Register (41 FR 11714) affecting the provisions relating to dissemination and security, and an extension of 90 days was announced for the submission of a supplemental plan covering these portions of the regulations.

The purpose of these explanatory instructions 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. 20.21

The Governor of each State is made 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 shall submit a plan on behalf of the State. That is, the plan will 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

Regulations Reference

complying with the regulations.

There are obvious difficulties in this approach. A State agency agency cannot commit all State and local agencies to follow 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 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 certifications 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 central State repository, these informational instructions will be implemented by means of contractual user agreements with those agencies or systems. Should there be systems at a local level which are not users 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. However, States 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 the interested agencies, public hearings, and conferences or workshops.

TIMING AND THE PLANNING PROCESS

Each State is required to submit its plan by March 16, 1976, and to submit a supplemental plan covering dissemination and security by June 17, 1976. The principal phases of each State's planning process

20.21

Regulations Reference

will be drafting, review by appropriate agencies, and the actual submission of the plan and supplemental plan.

Within 90 days of the receipt of the plan or supplemental plan, LEAA shall approve or disapprove the adequacy of the provisions of the plans. Evaluation of the plans 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 would have up to 90 days to revise the 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 28 C.F.R. Part 18.

20.25

KEY CONCEPTS IN THE PLANNING PROCESS

Definition of "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 the related term "administration of criminal justice."

"Criminal justice agency" means: (1) courts; (2) any 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(c)

"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 also includes criminal identification activities and the collection, storage, and dissemination of criminal history record information.

20.3(d)

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. Corporations and other private agencies which by contract perform important functions related by criminal justice should not be considered as government agencies. (See page .)

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. It need not, however, name the specific agency. Language which indicates that an agency is within a class of agencies authorized to perform a function of the administration of criminal justice will be sufficient authority.

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. Since most of the regulations do not have to be implemented until December 31, 1977, agencies should have time to acquire the necessary authority.

The definition of "administration of criminal justice" does not include crime prevention activities, nor criminal defense functions. Defense attorneys are therefore not eligible to receive records as criminal justice agencies. Neither are organizations that operate drug addiction treatment programs (or similar community programs) as a method of crime prevention (unless the treatment program was specifically charged by statute or executive order with the rehabilitation of offenders). These agencies may receive records, however [see the instructions on Section 20.21(b)(2)].

The term "executive order" is defined as an order by the President or the Chief Executive of a state which has the force of law and is published in a manner permitting regular public access thereto. Orders by local chief executives are not executive orders within the meaning of the regulations. 20.3(h)

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 have 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 regulation 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 who 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.

Regulations Reference

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.

Agencies Covered by the Regulations

All State and local agencies awarded 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 such systems handling 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 affected by the regulations. 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 funding be included under these 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 or dissemination of criminal history information. In other words, the mere receipt of criminal history record information by Agency B from Agency A does not bring Agency B under the coverage of these regulations, even if Agency A's system is federally funded. However, in such a case, Agency B, as a prerequisite to receiving information from Agency A, would have to sign a user agreement with Agency A and would be bound by the regulations to the extent that provisions of the regulations are incorporated in the user agreement. (See the Section of these instructions on "Limits on Dissemination" for more information.)

The following chart indicates the factors which govern the impact of the regulations on particular criminal justice agencies and the consequent procedures

Regulations Reference

required. To use the chart, find the column (1 through 13) that correctly indicates the combination of applicability criteria (upper left column) that characterizes your agency. For example, if your agency is LEAA-funded for maintenance of a criminal history record system, but neither receives records from other agencies nor disseminates records to other agencies or individuals, you would select column 9. If your agency does disseminate these records to other agencies or individuals, you would select either column 12 or 13. Once you have selected the correct column, simply read down the column to find which of the operational procedures (lower left column) are required of your agency ("x" indicates that the particular procedure is required). For example, if column 12 or 13 characterizes your agency, all of the listed operational procedures are required. If your agency does not receive LEAA funds, does not maintain criminal history records, but does receive such records from another agency and does not redisseminate them, column 4 would be applicable and would indicate that your agency would be bound to comply with the regulations as specified in the user agreement signed with the agency from which the records are received.

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
Control or approval of computer operations									X	X	X	X	X
Physical security/protection									X	X	X	X	X
Individual right of access									X		X	X	X

Regulations Reference

Definition of "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 regulations 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 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."' 20.3(b) and 20.20(a)

The regulations were written with the intent of covering collections of records containing historical references to an identifiable 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 is 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. The identification data does not have to include fingerprints, although the use of fingerprint-based identification to govern the entry of data into a criminal history file is strongly recommended as a means of insuring completeness and accuracy.

Although the regulations apply primarily to traditional "rap sheet" record systems, many other files or record systems maintained by criminal justice agencies may fall within the definition of criminal history record information. For example, the

Regulations Reference

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.

The definition of criminal history record information does not include intelligence or investigative information. Thus, the regulations do not apply to such information as suspected criminal activity, associates, hangouts, financial information, or ownership of property or vehicles. They also do not apply to information such as statistics derived from offender-based transaction statistics systems which do not reveal the identify of individuals. Criminal records of corporations are not included in the definition of criminal history record information since identifiable individuals are not involved.

Exclusions

The regulations specifically exclude certain types of information that might otherwise be included within the definition of criminal history record information. These specific exclusions include information contained in: 20.20(b)

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, complied chronologically and required by law or long-standing custom to be made public, if such records are accessed solely on a chronological basis.

3) Court records of public judicial proceedings.

4) Published court or administrative opinions.

5) Public judicial, administrative or legislative proceedings.

6) Records of traffic offenses maintained by State departments of transportation, motor vehicles or the equivalent thereof for the purposes of regulating the issuance, suspension, revocation, or renewal of driver's, pilot's or other operators'

Regulations Reference

licenses.

7) Announcements of executive clemency.

Exclusions (2) and (3) require explanation.

Original Records of Entry. The regulations do not apply to original source records prepared by criminal justice agencies to record, on a chronological basis, the occurrence of criminal events or transactions and basic facts about them. Examples include reports of crime scene investigations filled out by the investigating officer, individual arrest reports describing the arrest and circumstances surrounding it, and police blotters or equivalent arrest books used to record arrests chronologically and customarily made available to the press for inspection. The major function of such records is to provide current information on police activity and to guard against secret arrests, and this is the primary reason for the exclusion. However, an additional reason is that 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, and thus the public availability of such records does not present a significant danger of privacy abuse. 20.20(b)(2)

It must be clearly understood that these original source documents are excluded only if they are compiled and accessible solely on a chronological basis. If the documents are filed alphabetically, thereby allowing a search by name for retrieval of all such records related to a particular person, the collection of documents is no longer covered by the exclusion and becomes subject to the regulations. Likewise, any index to the documents that permits a search of the collection on the basis of name would, in conjunction with the documents, be criminal history record information and subject to the regulations. For example, in many areas the police blotter has been eliminated in favor of computerized booking systems which make it possible for private individuals or newsmen, upon submission of a specific name, to obtain, through a computer search, a history of the named 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.

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 routinely available to the public and

Regulations Reference

press only if they are 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 not possible to avoid the regulations by separating parts of a file or data system, such as by separating the name index from substantive records. Under the regulations, the physical distribution of the records is not relevant. As long as name access is permitted, and the access method effectively links the records together in retrieving them, the system falls under the definition of criminal history record information.

Court Records. The regulations also specifically exclude "court records of public judicial proceedings." The effect of this exclusion is to make the regulations inapplicable to information systems maintained by the judicial branch for the purpose of recording the processes and results of public court proceedings. It should be stressed that this does not affect the obligation of courts to report dispositions to systems maintained elsewhere, such as to central State repositories. 20.20(b)(3)

Examples of Systems Covered

The following table shows the extent of coverage of some typical record systems. It should be emphasized that the procedures required in the event a particular system qualifies for inclusion will vary, depending primarily on the extent of dissemination.

Exhibit 1. EXAMPLE 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, temporary 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
Local ordinance violations	Arrests/detentions for vagrancy, traffic, disorderly conduct, etc.	No, (only any CHRI contained therein)
Intelligence files	Investigative observations, associations	Yes
Alphabetical indexes to police case files	Name vs. case number	Yes, (need not be complete if only used internally)
M. O. files	Data on all persons arrested/convicted for a particular offense	No
Court case files	State vs._____, filed chronologically or by alphabetical index	No
State Judicial Information System	Data on case flow and defendant flow, court management information, court statistics, may also include CCH component or link to CCH	No
Court calendaring	Scheduled dates of actions, names of participants (excluding references to arrests or dispositions)	No
Alpha-indexed appellate decisions	Court opinions of public judicial proceedings	No

Regulations Reference

Public Disclosure of Criminal Proceedings

The regulations recognize that public announcements of ongoing developments in the criminal justice process should not be precluded. To quote the regulations, "Nothing in these regulations prevents a criminal justice agency from disclosing to the public criminal history record information related to the offense for which the individual is currently within the criminal justice system." This means that information may be released to the public concerning any aspect of an individual's case if the case is still pending or if he is still under the jurisdiction of any segment of the criminal justice system. This provision should be read in conjunction with Section 20.21(b), however, which provides that, after December 31, 1977, nonconviction data may not be given out for noncriminal justice purposes unless authorized by statute, ordinance, executive order or court order or rule. Since nonconviction data includes information relating to year-old arrests that have not resulted in a disposition and are not still under active prosecution (see page 29 of the instructions), information relating to such "pending" arrests may not be given out, absent appropriate legal authority (as set out in Section 20.21(b)(2)). If the individual is acquitted, or if charges are not brought or are dismissed or indefinitely postponed, information concerning such arrests also may not be released to noncriminal justice recipients unless authorized in accordance with Section 20.21(b)(2); this information could be obtained from court records, however.

20.20(c)

It is also permissible for a criminal justice agency to confirm certain matters of prior criminal 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.

Dissemination

Although "dissemination" is a key concept in the regulations, the regulations do not define the term. However, it can be interpreted to apply to the release or transmission 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 for purposes of the regulations. Further, reporting the occurrence of and the circumstances of a

Regulations Reference

criminal justice transaction is not dissemination. That is, the reporting of an arrest or other transaction, including dispositions, to a local or State repository, or to the FBI, is not dissemination. (See the last sentence of section 20.21(e)). Similarly, reporting data on a particular criminal charge 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; and prosecutors may use the information in preparing presentence reports or other reports for courts. Because of the "subject-in-process" nature of these uses of records, there will be no possibility that a transaction has occurred that is unknown to the agency transmitting the record. Hence, such transmissions need not be considered disseminations, and predissemination queries of the central State repository need not be made. It must be stressed that this interpretation applies only if the information passed from one agency to another relates solely to the criminal charge that is in process. If information is included that relates to other charges (for example, if a defendant's entire rap sheet is included in the file given by the police to the prosecutor) then a predissemination query of the central State repository is necessary to insure that the information relating to other charges is up-to-date. (See the section on Completeness and Accuracy for more information on predissemination queries.)

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 Section 20.21 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. — 20.22(b)(1) 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)

The only exception to this requirement is the matter of the dissemination limits set out in Section 20.21(b). Implementation of these limits need not occur until December 31, 1977, and there is no requirement that any explanation be given for failure to implement them prior to that time.

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) initiate steps to

Regulations Reference

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.

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. 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 timetables 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 responses the State may make to comply with the regulations. For example, if the plan calls for legislative action, an agency should be assigned the responsibility of drafting and sponsoring legislation. The plan should identify the agency responsible for overall implementation of the plan.

The State plan should not reflect details which would relate only to a single local agency. For example, the Police Department of the City of Buffalo, New York, may be subject to the regulations. Nevertheless, it will not be necessary to specify in the

Regulations Reference

plan Buffalo P.D.'s approach to implementing the regulations or a detailed schedule of implementation milestones for the department. The plan should present, however, the specific procedures the State and its agencies will establish to insure that covered local agencies are fully informed in a timely fashion concerning their responsibilities under the regulations. Such procedures may include: workshops, conferences, and mailing of these instructions and/or the State plan to local agencies.

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.

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."

Regulations Reference

To implement this provision, the regulations provide 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. 20.21(a)

"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 completeness requirements included in the regulations are made applicable to records maintained at such central repositories. 20.21(a)(1)

"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. 20.21(a)(2)

Limits on Dissemination

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 of nonconviction data for such non-criminal justice purposes as licensing, employment checks, security clearances and research. 20.21(b)

The regulations also require procedures for limiting the dissemination of juvenile records for non-criminal justice purposes. 20.21(d)

The regulations place no limits on dissemination of conviction data or data relating to pending cases.

Audits and Quality Control

Inherent in Section 524(b) of the Omnibus Crime Control and Safe Streets Act is the requirement that 20.21(e)

Regulations Reference

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

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 protection against unauthorized disclosures, protection of physical facilities, and selection, training and supervision of employees. 20.21(f)

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 the right. Included are procedures for access and challenge, 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 erroneous 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 20.21(a)(1)

Regulations Reference

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.

Central State 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 be 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. 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.

Regulations Reference

Reporting of Dispositions. 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 maintenence 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. 20.21(a)(1)

"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; 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. 20.3(e)

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 State at whatever level. The legislation should contain sufficient sanctions, including fines, penalties and audits, to assure that it is enforceable.

Reporting need not be directly to the central repository. The legislation in some States conceivably may 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

Regulations Reference

courts may report to a judicial administration unit at the State level, which acts as a satellite data collection center for the central repository. There may 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.

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 by means of a tracking number or some 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 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

Regulations Reference

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 be assigned at the point that a 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 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

Regulations Reference

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 is no intent to require that agencies go back into old 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. 20.23

The plan should include some method of insuring implementation of the 90-day reporting requirement or whatever shorter 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 detailed provisions of audit procedures are discussed further in the Section concerning audit and quality control. 20.21(e)

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 few weeks.

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

Regulations Reference

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(b) 20.3(k)

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)

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. But it is not applicable 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, the

Regulations Reference

procedures might appropriately exempt from the query requirement enumerated disseminations, such as police 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." 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 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. 20.21(a)(1) 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

Regulations Reference

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 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 a police investigative system, 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 nonexistence of a criminal history record, and thus such a confirmation may not be communicated to anyone who would not be eligible to receive the records themselves. 20.21(b)

The plan must set forth operational procedures to limit dissemination of criminal history record information in the following manner: 20.21(c)(2)

Regulations Reference

Conviction Data and Pending Charges

The regulations place no limits on the dissemination of conviction data, that is, information indicating that an individual pleaded guilty or nolo contendere to criminal charges or was convicted. Nor do they prohibit the release of information concerning cases that are pending in some stage of processing or prosecution. All such information may be disseminated, both to criminal justice agencies and to noncriminal justice recipients, to the full extent that such dissemination is legal (that is, not prohibited by law) in particular states and local governmental jurisdictions. Of course, any state or local law or order limiting dissemination of such data would not be affected by the regulations. 20.21(b) 20.20(c)

Nonconviction Data

The only dissemination limits imposed by the regulations relate to "nonconviction data," defined by Section 20.3(k) to include information disclosing that (1) the police have elected not to refer a matter for prosecution, (2) a prosecutor has elected not to commence criminal proceedings (3) proceedings have been indefinitely postponed, (4) all dismissals (5) all acquittals, and (6) arrest records without dispositions if a year has elapsed and no conviction has resulted and no active prosecution is pending. The term thus includes, among others, the following dispositions (or their equivalents under applicable state or local law): no paper, nolle prosequi, indefinitely postponed, acquittal on the merits, acquittal due to insanity, acquittal due to mental incompetence, charge dismissed, charge dismissed due to insanity, charge dismissed due to mental incompetency, dismissed -- civil action, and mistrial -- defendant discharged. Where prosecution is deferred or postponed in order to divert the defendant to a treatment alternative program, such a case is still actively pending and the deferral disposition is not considered nonconviction data until the charges are ultimately dismissed. 20.3(k)

In order for a year-old arrest record with no recorded disposition to be still under "active prosecution," the case must be still actively in process, that is, the first step, such as arraignment, must have been completed and the case docketed for court trial. Where prosecution has been officially deferred to divert the defendant to a treatment alternative program, such a deferral is a disposition and should be

Regulations Reference

entered on the record.

Effective on December 31, 1977, dissemination of nonconviction data must be limited to:

1) "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 instructions related to Section 20.3(C), page 3.) — 20.21(b)(1)

2) "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 violations thereof." — 20.21(b)(3)

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 system development and operation would also be included here.

3) "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." — 20.21(b)(4)

Under this exception, any good faith researchers, including private individuals, would be permitted to use criminal history record information for research purposes. As with the agencies designated in Section 20.21(b)(3), researchers would be bound by an agreement

Regulations Reference

with the disseminating criminal justice agency and would thereby 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. "Certification" criteria would have been extremely difficult to draft and would have led inevitably 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 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.

4) Individuals and agencies for any purpose authorized by statute, ordinance, executive order, or court rule, decision or order, as construed by appropriate State or local officials or agencies. — 20.21(b)(2)

The intent of this provision is to permit the dissemination of nonconviction data when authorized either explicity or impliedly by one of the legal means specified in the previous paragraph. Thus, such data may be distributed pursuant to a licensing statute or ordinance that requires license applicants to be of good moral character, if the statute or ordinance has been construed by appropriate authority (by a court decision or an Attorney General's opinion, for example) to require or permit a review of nonconviction records in making the determination of good moral character. Similarly, where a statewide law, such as a "public

Regulations Reference

records" law, has been construed by the State courts or the Attorney General to authorize public access to all public records, including criminal records, such a law would qualify as statutory authority under the regulations. Authority might also be found in a State or federal executive order authorizing civil service suitability investigations, including a check of FBI or State bureau of identification fingerprint files and written inquiries to appropriate law enforcement agencies.

For purposes of this provision, an "ordinance" is the enactment of the legislative body of a local governmental unit, such as a county, city or municipality.

Finally, a court rule, order or decision requiring or authorizing the availability of criminal records to individuals or agencies, or classes of individuals or agencies, would be appropriate authority under the regulations.

The regulations also specifically authorize the dissemination of criminal history record information, including nonconviction data, for purposes of international travel or status, such as the granting of citizenship or the issuance of visas.

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.

Effective Date

It should be noted that the limitations on dissemination do not become effective 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 or other action needed to comply with the regulations. It should also be noted that there is no requirement for states to explain why implementation is not accomplished prior to December 31, 1977. 20.21(b)

Juvenile Records

Dissemination of juvenile records to non-criminal justice agencies is prohibited except where the 20.21(d)

Regulations Reference

dissemination takes place pursuant to (1) a good faith research agreement, (2) a contract to provide criminal justice services to the disseminating agency, or (3) a statute, court order or rule or court decision specifically authorizing juvenile record dissemination. It is important to understand clearly that these authorizations must expressly mention juvenile records; authority to receive criminal history records will not suffice. 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, because such authority is based upon an executive order and does not now expressly authorize access to juvenile records.

Another important point about this section of the regulations is that it must be strictly construed as nothing more than a limitation on dissemination of juvenile records. It applies to particular records only after there has been an adjudication that a youth is delinquent or in need of supervision (or the equivalent). The provisions of the regulations concerning completeness and accuracy, right of access for challenge and other matters do not apply to juvenile records; these issues must be resolved in future legislation or regulations.

User Agreements

The regulations require each State plan to insure that after December 31, 1977, dissemination of nonconviction data 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. 20.21(b)

In practice, this means that, whenever a criminal justice agency subject to the regulations receives a request for a record that includes nonconviction data, the agency must, before releasing the record, determine that the requesting agency or individual is (1) an eligible recipient and (2) aware of and subject to the

Regulations Reference

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) restricting the use of criminal history records to the purposes for which they were made available. All recipients must also 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 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 at least one certified criminal justice agency, preferably a central State repository.

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 the

Regulations Reference

limits on use and dissemination 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 covered by the regulations 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 written or 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.

Validation of Requester's Authority

Before any dissemination takes place, disseminating agencies must be certain that the potential recipient is an agency permitted to receive information under the regulations. — 20.21(b) and 20.21(f)(6)

If a potential noncriminal justice recipient claims to be authorized to receive information pursuant to a statute, ordinance, executive order, or court order, rule or decision, and the disseminating agency is not certain that the claimed basis is proper authority for dissemination, it should refuse to release the information pending an opinion by an appropriate State or local official or agency. As in the case of user agreements, discussed above, criminal justice agencies may accept written or oral representations from requesting agencies or individuals that their authority to receive criminal history records has been reviewed

Regulations Reference

and approved by the central State repository or by another criminal justice agency.

Expiration of Availability

The regulations state that after December 31, 1977, criminal history record information concerning the arrest of an individual may not be disseminated to a non-criminal justice agency or individual [execpt under Subsection 20.21(b)(2), (3) or (4)], 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 considered to be still active.) The arrest and disposition reporting process identified previously in these instructions should include 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(b) 20.3(k)

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

Access by the Military

Section 504 of title 10 of the United States Code 20.21(b)(2)

Regulations Reference

provides that no person who has been convicted of a felony may enlist in the armed forces, except with special permission. Since implementation of this statute requires armed forces recruiters to review only conviction records, this statute is not adequate authority for the dissemination of nonconviction data. Further, since the statute does not contain any specific reference to juvenile records, it does not satisfy the requirements of Section 20.21(d) and hence may not be relied upon as authority for allowing military recruiters to access juvenile records. 20.21(d)

AUDITS AND QUALITY CONTROL

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 a 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 repository is 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 estimated 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 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.

Regulations Reference

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 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

20.21(a)(2)

Regulations Reference

is disseminated and the record from which the information was extracted.

The regulations require logging of information released. When the response to an inquiry is "no record," LEAA has concluded that such a response would not require logging.

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 form 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 notifications were released.

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 agency to be held responsible for conducting 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.

20.21(e)

The auditing agency should inform the audited agency fully of its findings. The audit findings should also be available for LEAA inspection, upon request.

The annual audit should encompass all elements relative to the adherence of these regulations. Sampling procedures should be established for the

Regulations Reference

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.

Complete logs of dissemination maintained at each point authorized to release criminal history record data are necessary to support annual audits. 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 specify a number of requirements to ensure the confidentiality and security of criminal history record information. These requirements are set forth in general terms and are to be implemented by security standards established by each State by legislation or by regulations issued or approved by the Governor of the State. The plan need not delineate the details of the standards. However, it should describe the essential elements of the standards and should describe how the State intends to implement and enforce them. 20.21(f)

This Section of the regulations applies to both manual and computerized record systems, although some requirements apply only to computerized systems. The regulations permit the operation of shared systems serving various users including criminal justice agencies. Although a criminal justice agency must be ultimately responsible for compliance with the regulations, this can be accomplished by review and

Regulations Reference

approval of procedures developed by another agency and monitoring the implementation of such procedures to assure compliance with the regulations. For example, the operational programs and procedures for computerized data processing required by Section 20.21(f)(3) may be developed and implemented by a noncriminal justice EDP division operating a shared computer system with a criminal justice component, provided the procedures are approved by the participating criminal justice agencies and they are afforded the right to monitor the operations of the system to assure that the procedures are being properly implemented.

Unauthorized Access

The regulations require each State to develop standards to protect against unauthorized access to criminal history record information systems. These protective procedures must be developed for all systems within the State that are covered by the regulations, both computerized and manual systems. The standards must address the issue of authority to access criminal history record information or to modify, change, update, purge or destroy such information, and must be designed to effectively restrict such access and activities to authorized criminal justice personnel and other authorized persons who provide operational support such as programing or maintenance. 20.21(f)(2)

The standards should cover access to:

1) Physical facilities where any equipment or data is located or stored;

2) All parts of the physical portion of the system; in the case of computer systems this inlcudes terminals and any other peripheral devices from which data may be obtained as well as any storage devices whether interconnected to the computer or not; and

3) System documentations, including such things as programs, flowcharts and security manuals.

The standards should deal with different methods of access, including direct terminal access, indirect access through an agency with terminal access, and physical (personal) access, and should define:

1) Agencies and individuals permitted access;

Regulations Reference

2) Purposes of access;

3) Accountability for data obtained; and

4) Mechanisms for controlling access.

For both manual and automated systems, procedures must be implemented that will assure that persons authorized to have direct access to information (that is, access to the data base itself rather than indirect access through another person or agency) is held accountable for the physical security of any accessed information under their control or in their custody and the protection of such information from unauthorized disclosure or dissemination. 20.21(f)(3)(A)(vi) 20.21(f)(4)(c)

Computer Systems

The regulations set out in some detail the operational procedures that must be developed to protect computer systems against unauthorized access. Compliance with these provisions of the regulations will require direct involvement and final decision-making powers for criminal justice agencies in developing policy governing the operation of a computer used to handle criminal history record information. Where the computer is "owned" by a criminal justice agency and the agency's staff is responsible for all operations, the required policy authority is present and will be exercised directly. However, where the computer center is managed by a noncriminal justice agency, such as an EDP division that does not meet the test of being a criminal justice agency, the regulations require that operational policies and procedures must be developed or approved by the participating criminal justice agencies and such agencies must have the right to audit, monitor and inspect the procedures to assure that they are being implemented in a manner agreeable to them and in compliance with the regulations. Thus, it is possible to satisfy the regulations with a system that is neither dedicated nor under the direct control of a criminal justice agency, provided the criminal justice agency users have the right and capability of assuring that operational policies and procedures are adequate to achieve an acceptable level of security. This means that the criminal justice agency or agencies so designated must be able to inspect the operations and review procedures as well as have a mechanism for initiating action to change an unsatisfactory operation. The plan should indicate the specific criminal justice agency or agencies which have 20.21(f)(3)(A)

Regulations Reference

or will have this authority over the operation of the computer used by the central State repository if a shared computer environment is envisioned.

Software and Hardware Designs

The regulations provide that computerized systems must employ "effective and technologically advanced software and hardware designs" to prevent unauthorized access to criminal history record information. It is not useful or desirable to attempt to define all of the technological design features which would achieve the objective of preventing unauthorized access, either in the regulations or in the plans to be prepared. Rather, the State should describe the functions related to security which will be achieved by the system design. 20.21(f)(1)

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 telecommunication codes, would be sufficiently difficult to reconstruct so as to permit such transmissions unless the transmitting agency has reason to doubt the security of the medium. While there is no requirement in the regulations for scrambling or other encryption of transmissions, the transmitting agency must assure itself that the receiving site sustains a reasonable level of security.

System design can be one way of minimizing the likelihood of unauthorized access, although the system design cannot be expected to totally prevent unauthorized access. The institution of these designs should be aimed at both prevention and notification of attempts to penetrate the system.

Prevention is accomplished by making it difficult for an unauthorized user or terminal to access the files. Disign features would include techniques such as:

1) Terminal identification numbers which are checked by the computer before responding to an inquiry;

2) Software which limits terminal access to only certain files or data (depending on eligibility criteria);

Regulations Reference

3) Further restrictions on terminals used for making changes or deletions, such as limiting this function to specific terminals in well-controlled environments;

4) User authentication software or hardware devices; and

5) Erasing or eliminating residual information in unprotected storage or at remote terminals.

In addition to preventing unauthorized inquiries of criminal justice information systems, the regulations require procedures to prevent unauthorized tampering with information in the system. This includes procedures to ensure that noncriminal justice terminals may not modify, change, update or otherwise affect the storage media used for criminal history record information and that such informatin may not be destroyed except by specifically designated terminals under the direct control of the agency that created and contributed the record or an agency with the responsibility for maintaining it. This would apply to any form of storage, including tapes, discs, core memory in the computer, or any peripheral storage devices. 20.21(f)(3)(A)

Computerized systems must employ operational software programs to protect against such unauthorized inquiries, modifications or destruction of records and to record and report all attempts to penetrate the system for such an unauthorized purpose. This special software must be accorded a higher level of security than the normal operations or application software and should be known only to limited individuals, either in a criminal justice agency or in the programing agency responsible for system control, in which case an agreement must be executed to provide maximum security for this software. The purpose of these programs should be to alert system operators of attempts to penetrate the system. Software should be designed to detect and display attempts by unauthorized users or terminals. Other desirable features would include automatic cutoff of terminals used in violation of security requirements, load monitoring to determine unusual activity, and similar detection techniques.

For further guidelines in developing such procedures, planners may wish to consult Project SEARCH Technical Report No. 6, entitled "Criminal Justice Computer Hardward and Software Security Considerations."

Regulations Reference

Personnel

The regulations distinguish two levels of authority to be assigned to criminal justice agencies relative to personnel assignment. First, where employees of a criminal justice agency (employees include civil service staff, contract employees, and anyone else who is totally supervised by the agency) are the only persons who handle data or files, it is assumed that the requisite authority is achieved. Of primary interest then is the instance where personnel of a noncriminal justice agency are involved. In such cases, the designated criminal justice agency must have the power to exclude, for good cause, individuals from having direct access to criminal justice records. This power is limited to a veto over personnel assignment, and does not imply any right to make personnel selections. It would apply to secretaries, guards, maintenance personnel and computer operators who work in areas where criminal justice records are stored and who have the opportunity and capability to access the records, as well as individuals whose duties clearly require direct access (file clerks, applications programers, etc.). 20.21(f)(4) 20.21(F)(4)(A)

There is no intent to conflict with civil service practices already in existence for the selection process, and it may well be that candidates are screened and presented to the criminal justice agency by another agency of government. However, the criminal justice agency must make the final decision as to the acceptability of the person and must be able to initiate or cause to be initiated administrative action to transfer or remove persons who violate security requirements or other procedures required by the regulations. 20.21(f)(4)(B)

Where the system is operated by a criminal justice agency, the regulations essentially call for a personnel clearance system. The plan should describe such a system to be used in agencies which have the responsibility for maintaining or disseminating criminal history record 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

Regulations Reference

the need to know.

The use of noncriminal justice personnel (such as individuals from other government agencies or contractor services) is permissible under the regulations for purposes of system development and operation, including programing and data conversion. Access to criminal history data by these individuals is authorized by Section 20.21(f)(4)(E), but only to the extent that such access is "essential to the proper operation of the criminal history record information system." 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 fulltime 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 escorts, equipment access limitations, etc., can be used where appropriate.

Physical Security

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 central repositories of information from fire, flood, wind, theft, sabotage, or other natural or manmade hazards or disasters. 20.21(f)(3)(A)(vii) 20.21(f)(4)(D)

Agencies administering central repositories of criminal justice information 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 central repository 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 may include: physical limitations on access; security storage for information

Regulations Reference

media; heavy-duty non-exposed walls; perimeter barriers; adequate lighting; detection and warning devices; and monitoring devices such as closed circuit television. The plan should clearly outline these procedures or others which will accomplish an equivalent level of security for the physical facilities of central repositories which contain criminal history information.

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

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. 20.21(g) 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 identify, 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 issues at the minimum. 20.21(g)(1)

Verfication 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

Regulations Reference

required where the individual is well known to the official responsible for verifications. 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 identity verification.

Rules for Access and Challenges

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 made, 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 or parent or guardian, 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 reviw 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 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. Although normally it will be permissible to require that the review take place at an

20.21(f)(1)

Regulations Reference

agency that has custody or control of the record, this would, of course, not be permissible where complete records are 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.

The plan should specify how information maintained by the central repository may be reviewed by individuals throughout the State. In large States, this will probably require a statement of intent to designate certain local criminal justice agencies as places where State criminal histories may be sent for review.

The plan need not specify how each local agency maintaining criminal history information will meet its obligation to provide the right of review "without undue burden." The obligation, nonetheless, exists, and local agencies faced with requests for review from individuals located some distance from the agency may have to seek the cooperation of other agencies close 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 42 USC Sec. 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. 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. It is necessary to release only a copy of that portion of the record that is challenged.

20.21(g)(1)

Any attempt by employers to subvert 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

Regulations Reference

individual attesting to the lack of a record. Such a "good character" letter would be confirmation of the existence or nonexistence of criminal history record information, is defined to be dissemination, and is therefore limited by Section 20.21 (c)(2). (See the prior discussion of this subject in the section on Limits on Dissemination.)

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.

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

The regulations state that the plan must provide for "administrative review and necessary correction 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, he is entitled to an audit of appropriate source documents to determine the validity of his challenge. 20.21(g)(2)

The plan should specify time limits for the initiation of the audit and for the determination after the audit. It should also require that published agency rules shall state the identity or titles of the individual or official with responsibility for

Regulations Reference

administratively reviewing record challenges.

Administrative Appeal

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. 20.21(g)(3)

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, or provide for the establishment of such procedures.

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. 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

Regulations Reference

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

The regulations provide that records found to be incorrect or incomplete must be appropriately corrected, and 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.)

20.21(g)(2)
20.21(a)(2)
20.21(g)(4)

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

20.21(g)(5)

Regulations Reference

have received inaccurate information. Earlier in this Section it was stated that such logs should be maintained for one year.

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 juvenile records nor intelligence and investigative information. Nor is he entitled to review substantive reports compiled 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 a correctional institution, but not medical records and other records of treatment at the institution.

20.21(g)(6)

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 criminal 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 as Minimum Requirements

The procedures set out above should be regarded as minimum requirements and not as limitations on the right of States to provide more extensive procedures. States may, for example, provide for review of a minor's record by his parent or legal guardian, may provide for a more extensive administrative review procedure, and may provide for the notification of non-criminal justice agencies in the event a record is found to be erroneous. None of these additional rights would be in conflict with the regulations.

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. The certification also must include a listing of all categories of non-criminal justice uses of criminal history record information in the State.

20.22

20.23

20.22(b)(5)

A certification consists of:

1) A checklisk 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 regulations and what has been done about them.

4) A listing of all categories of non-criminal justice dissemination authorized in the State.

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

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.

The several separate components of the certification that are specifically required by the

Regulations Reference

regulations are discussed below.

ACTIONS TAKEN AND DESCRIPTION OF SYSTEM CAPABILITY

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." 20.22(b)(1)

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 regulations 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)

A 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 Ref.	OPERATIONAL PROCEDURES	Now Implemented	Reasons For Non-Implementation: Cost	Technical	Lack of Authority	Estimated Implementation Date
	Completeness and Accuracy					
20	Central State Repository:					
21	Statutory/Executive Authority	___	___	___	___	___
21	Facilities and Staff	___	___	___	___	___
	Complete Disposition Reporting in 90 days from:					
24	Police	___	___	___	___	___
24	Prosecutor	___	___	___	___	___
24	Trial Courts	___	___	___	___	___
24	Appellate	___	___	___	___	___
24	Probation	___	___	___	___	___
24	Correctional Institutions	___	___	___	___	___
24	Parole	___	___	___	___	___
	Query before Dissemination:					
26	Notices/Agreements--Criminal Justice	___	___	___	___	___
	Systematic Audit:					
25	Delinquent Disposition Monitoring	___	___	___	___	___
37	Accuracy Verification	___	___	___	___	___
38	Notice of Errors	___	___	___	___	___
28	Limits on Dissemination*					
	Contractual Agreements/Notices and Sanctions in Effect For:					
30	Criminal Justice Agencies	___				___
	Non-Criminal Justice Agencies					
31	Granted Access	___				___
30	Service Agencies Under Contract	___				___
30	Research Organizations	___				___
35	Validating Agency Right of Access	___				___
	Restrictions On:					
32	Juvenile Record Dissemination	___				___
28	Confirmation of Record Existence	___				___
36	Dissemination Without Disposition	___				___
37	Audits and Quality Control					
	Audit Trail:					
38	Recreating Data Entry	___	___	___	___	___
38	Primary Dissemination Logs	___	___	___	___	___
40	Secondary Dissemination Logs	___	___	___	___	___
39	Annual Audit	___	___	___	___	___

* There is no requirement that a reason be given for nonimplementation of these procedures before December 31, 1977.

EXAMPLE CERTIFICATION FOR A CENTRAL STATE REPOSITORY (Continued)

Instructions Page Ref	OPERATIONAL PROCEDURES	Now Implemented	Reasons For Non-Implementation: Cost	Technical	Lack of Authority	Estimated Implementation Date
	Security					
40	Executive/Statutory Standards	___	___	___	___	___
41	Prevention of Unauthorized Access and Tampering:					
43	Hardware/Software Designs for Computer Systems	___	___	___	___	___
41	Designs for Manual Systems	___	___	___	___	___
	Criminal Justice Agency Authority:					
42	Computer Operations Policy Development or Approval	___	___	___	___	___
45	Approval and Clearance of Personnel	___	___	___	___	___
	Physical Security:					
46	Theft, Sabotage	___	___	___	___	___
46	Fire, Flood, Other Natural Dangers	___	___	___	___	___
45	Employee Training Program	___	___	___	___	___
47	Individual Right of Access					
48	Rules for Access	___				
48	Point of Review and Mechanism	___				
50	Challenge by Individual	___				
50	Administrative Review	___				
50	Administrative Appeal	___				
52	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.)

SAMPLE CERTIFICATION FOR AN AGENCY OTHER THAN THE CENTRAL STATE REPOSITORY

Instructions Page Ref.	OPERATIONAL PROCEDURES	Now Implemented	Reasons For Non-Implementation: Cost	Technical	Lack of Authority	Estimate Implementation Date
20	Completeness and Accuracy					
	Complete Disposition Reporting from:					
24	Police	____	____	____	____	____
24	Prosecutor	____	____	____	____	____
24	Trial Courts	____	____	____	____	____
24	Appellate Courts	____	____	____	____	____
24	Probation	____	____	____	____	____
24	Correctional Insitutions	____	____	____	____	____
24	Parole	____	____	____	____	____
26	Query Before Dissemination	____	____	____	____	____
	Systematic Audit:					
25	Delinquent Disposition Monitoring	____	____	____	____	____
37	Accuracy verification	____	____	____	____	____
28	Limits on Dissemination*					
	Contractual Agreements/Notices and Sanctions in Effect For:					
30	Criminal Justice Agencies	____				____
31	Non-Criminal Justice Agencies Granted Access	____				____
30	Service Agencies Under Contract	____				____
30	Research Organizations	____				____
35	Validating Agency Right of Access	____				____
	Restrictions On:					
32	Juvenile Record Dissemination	____				____
28	Confirmation of Record Existence	____				____
36	Dissemination Without Disposition	____				____
37	Audits and Quality Control					
	Audit Trail:					
38	Recreating Data Entry	____	____	____	____	____
38	Primary Dissemination Logs	____	____	____	____	____
40	Secondary Dissemination Logs	____	____	____	____	____

* There is no requirement that a reason be given for nonimplementation of these procedures before December 31, 1977.

SAMPLE CERTIFICATION FOR AN AGENCY OTHER THAN THE CENTRAL STATE REPOSITORY (Continued)

Instructions Page Ref.	OPERATIONAL PROCEDURES	Now Implemented	Reasons For Non-Implementation: Cost	Technical	Lack of Authority	Estimate Implementation Date
40	Security					
40	Executive/Statutory Standards	____	____	____	____	____
41	Prevention of Unauthorized Access and Tampering:					
43	Hardware/Software Designs for Computer Systems	____	____	____	____	____
41	Designs for Manual Systems	____	____	____	____	____
	Criminal Justice Agency Authority:					
42	Computer Operations Policy Development or Approval	____	____	____	____	____
45	Approval and Clearance of Personnel	____	____	____	____	____
	Physical Security:					
46	Theft, Sabotage	____	____	____	____	____
46	Fire, Flood, Other Natural Dangers	____	____	____	____	____
45	Employee Training Program	____	____	____	____	____
47	Individual Right of Access					
48	Rules for Access	____				
48	Point of Review and Mechanism	____				
50	Challenge by Individual	____				
50	Administrative Review	____				
50	Administrative Appeal	____				
52	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 Agency submitting certification.)

Regulations Reference

AUTHORIZING ORDERS AND LEGISLATION

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, where the Governor has authority to issue executive orders to further compliance with the regulations, necessary executive orders should have been issued by the time of plan submission. 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 --for example, drafted and introduced, undergoing hearings, awaiting the convening of a biennial legislative session.

20.22(b)(2)

PROGRESS TOWARD PROBLEM RESOLUTION

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.

20.22(b)(3)

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.

AUTHORITY FOR NON-CRIMINAL JUSTICE USES

Regulations Reference

The certification requires a "listing setting forth categories of non-criminal justice dissemination. This section of the certification is required by Section 20.21(b)(2) which limits the dissemination and use of nonconviction data for non-criminal justice purposes to those instances where dissemination and use is authorized by statute, ordinance, executive order, or court rule, decision or order. This section is discussed earlier in these guidelines.

20.22(b)(5)

The certification need not set forth citations of all statutes, executive orders and other authority under which dissemination is authorized. All that is required is a listing of categories of non-criminal justice dissemination, indicating the classes of recipients, the types of information available, the purposes for which it may be used and an indication of the type of authority (i.e., statute, executive order, court order or whatever).

This information need not be supplied until the final certification is submitted on or before December 31, 1977.

Regulations Reference

Section 4

PENALTIES FOR NON-COMPLIANCE WITH THE REGULATIONS

Agencies may be subject to the penalties of the Act for knowing and willful failure to comply with any of the following requirements: 20.25

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.

LEAA will recommend violations for court imposition of fines (which may be up to $10,000) only in cases of clearly willful and knowing violations.

FAILURE TO SUBMIT ADEQUATE PLAN OR CERTIFICATIONS

Submission of the plan and certifications is 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.

Regulations Reference

FAILURE TO COMPLY WITH SPECIFIC PROVISIONS

The Effect of Certification

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. 20.23

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

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 may subject the agency to the sanctions under the regulations and Act. 20.23

END