



**ARIZONA PLAN
for the
SECURITY AND PRIVACY
of
CRIMINAL HISTORY RECORD INFORMATION**

Approved September 8, 1977

47772

**Arizona State Justice Planning Agency
5119 N. 19th Avenue, Suite M
Phoenix, Arizona 85015**

Revised December 2, 1977



**ARIZONA PLAN
for the
SECURITY AND PRIVACY
of
CRIMINAL HISTORY RECORD INFORMATION**

Approved September 8, 1977

Arizona State Justice Planning Agency
5119 N. 19th Avenue, Suite M
Phoenix, Arizona 85015

Revised December 2, 1977

NOV 17 1977

JUN 5 1978

ACQUISITIONS



UNITED STATES DEPARTMENT OF JUSTICE
LAW ENFORCEMENT ASSISTANCE ADMINISTRATION
WASHINGTON, D. C. 20531

SEP 8 1977

Mr. Ernesto G. Muñoz, Executive Director
Arizona State Justice Planning Agency
Office of Attorney General
Continental Plaza Building, Suite M
5119 North 19th Avenue
Phoenix, AZ 85051

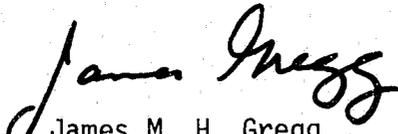
Dear Mr. Munoz:

This is with reference to the Arizona Privacy and Security plan.

Pursuant to the Department of Justice Criminal Justice Information Systems Regulations, (28 CFR Part 20), LEAA has completed its review of the additional documentation submitted in response to our request.

On the basis of this review, LEAA is pleased to inform you that the Arizona Privacy and Security plan is now approved.

Sincerely,


James M. H. Gregg
Acting Administrator



CONTENTS

	Page
I. INTRODUCTION	
A. Scope and Authority	1
B. Applicability	1
C. Notice	1
D. Limitations	2
E. Effective Dates	2
F. Responsibilities for Implementation of this Plan	2
G. Penalties	3
H. The General Requirements of the Regulations	3
II. DEFINITIONS	
A. Definitions Contained in 28 CFR 20	5
B. Arizona Definitions	6
III. DESCRIPTION OF THE ARIZONA CDS FOR CRIMINAL JUSTICE	
A. Background	7
B. ACJIS at a Glance	7
C. Information Contained in Automated Systems	9
D. Manual Record Systems	10
E. Automation — a Gradual Process	10
F. System Management — the Security and Privacy Council and Arizona Rules for Security and Privacy	11
IV. OBJECTIVES OF THIS PLAN	
A. Objective #1 — Completeness and Accuracy	13
B. Objective #2 — Limits on Dissemination	18
C. Objective #3 — Audits and Quality Control	31
D. Objective #4 — Security	35
E. Objective #5 — Individual Rights of Access and Review	43

CONTENTS (Continued)

V. CERTIFICATION

- A. Certification Statement 49
- B. Dissemination Authorized to Non-Criminal Justice Agencies 49

VI. ATTACHMENTS

- A. Federal Register Vol. 40, No. 98 (28 CFR 20) of May 20, 1975,
amended as of March 19, 1976 51
- B. ARS 41-1750 65
- C. ARS 41-1751 67
- D. Final Disposition Report Form 68
- E. Department of Public Safety — Criminal Identification
Section Report of Record Search Form 70
- F. Request for Record Information Form 71
- G. Review of Criminal Offender Record Information Form 72
- H. Exceptions Taken to Criminal Offender Record Information
Form 73
- I. Notice of Results of Audit of Criminal Offender Record
Information Form 74
- J. Certification Statements Form 75
- K. Criminal History Record Information User Agreement Form 78
- L. ARS 41-2201-2206 80

RECORD OF CHANGES

After removing obsolete pages and filing revised pages, initial and date the block following the change number.
Request any missing changes from your distribution point.

Change No.	Initial	DATE FILED									
1			35			69			103		
2			36			70			104		
3			37			71			105		
4			38			72			106		
5			39			73			107		
6			40			74			108		
7			41			75			109		
8			42			76			110		
9			43			77			111		
10			44			78			112		
11			45			79			113		
12			46			80			114		
13			47			81			115		
14			48			82			116		
15			49			83			117		
16			50			84			118		
17			51			85			119		
18			52			86			120		
19			53			87			121		
20			54			88			122		
21			55			89			123		
22			56			90			124		
23			57			91			125		
24			58			92			126		
25			59			93			127		
26			60			94			128		
27			61			95			129		
28			62			96			130		
29			63			97			131		
30			64			98			132		
31			65			99			133		
32			66			100			134		
33			67			101			135		
34			68			102			136		

ABSTRACT

This Plan for the Security and Privacy of Criminal History Record Information provides for the implementation of certain sections of Subpart B to Federal Regulations 28 CFR 20 issued by the U. S. Department of Justice on May 19, 1975. The Plan applies principally to those state and local criminal justice agencies which, since July 1, 1973, have received financial assistance from the Law Enforcement Assistance Administration for the collection, storage, and dissemination of criminal history record information. The Plan provides guidance to state and local criminal justice agencies for the following:

- Assuring the completeness and accuracy of criminal history records;
- Limitations on the dissemination of criminal history information;
- Audits and quality control procedures;
- Physical security of record keeping facilities; and
- Individual rights to access and review.

The general requirements of the Regulations are that all affected agencies must:

- Initiate procedures to assure the completeness and accuracy of criminal history records in their custody; (This must be in effect by March 1, 1978.)
- Institute procedures, by March 1, 1978, to query the State Central Repository, located at the Arizona Department of Public Safety to assure that the most current information is being used or disseminated;
- Restrict the dissemination of criminal history record information and maintain a record of the dissemination of criminal history record information in sufficient detail to provide a clear audit trail and to provide a method for informing and providing corrected information to recipients of inaccurate or incomplete information;
- Take certain measures to assure the integrity of computer files and the physical security of record keeping facilities;
- Permit an annual audit, under auspices of the Comprehensive Data System (CDS) Policy Board, of procedures for maintaining the security of records and controlling the dissemination of information;
- Institute not later than March 15, 1976, procedures whereby an individual may review his criminal record and challenge inaccurate or incomplete information.

Except for the individual's right to challenge his own record, which became effective on March 15, 1976, this Plan does not prescribe procedures to be implemented; rather it presents guidelines for developing suitable procedures to be placed in effect not later than March 1, 1978.

The Security and Privacy Council, established under the authority of the CDS Policy Board, has the responsibility for reviewing procedures to assure that minimum standards for security and privacy are met.

This Plan received final approval by the Law Enforcement Assistance Administration on September 8, 1977.

**SECTION I
INTRODUCTION**

Section I INTRODUCTION

A. SCOPE AND AUTHORITY

This Plan for the security and privacy of criminal history record information provides for the implementation of Subpart B of Federal Regulations 28 CFR 20 hereinafter referred to as the Regulations. A copy of the Regulations is appended hereto marked Attachment A. This Plan was prepared under authority of the Governor of Arizona letter of July 14, 1975.

The provisions of Subpart C of the regulations are implemented by Section IX of the ARIZONA COMPREHENSIVE DATA SYSTEM FOR CRIMINAL JUSTICE MASTER PLAN of May, 1975, to which this plan should be considered a companion and supplement.

B. APPLICABILITY

1. Applicability of Subpart B of the Regulations

Agencies who satisfy the following criteria are subject to Subpart B of the Regulations:

- a. Have received funds since July 1, 1973, specifically for the collection, storage, and dissemination of criminal history record information; or
- b. Have, through use of LEAA funds received since July 1, 1973, established or improved manual record keeping systems or have established automated or partially automated manual record keeping systems which contain criminal history record information.

2. Applicability of Subpart C of the Regulations

Subpart C of the Regulations is applicable to those agencies who do not fit the criteria of I.B.1. above, but who are now, or who may become subscribers to the Arizona Criminal Justice Information System (ACJIS) network and who are, or may become, parties to a Criminal History Record Information User Agreement with the Arizona Department of Public Safety for the receipt of criminal history information by other means, but only to the extent that those agencies utilize the services of the National Crime Information Center-Computerized Criminal History (NCIC-CCH) information system.

C. NOTICE

This Plan serves as notice to the covered agencies of their obligations under Subpart B of the Regulations.

The agencies who have received grants or subgrants through the Arizona State Justice Planning Agency since 1969 for the collection, storage, or dissemination of criminal history record information are:

- The Arizona Department of Public Safety
- The Arizona Department of Corrections
- The Phoenix Police Department
- The Tucson Police Department
- The Maricopa County Sheriff's Department
- The Pima County Sheriff's Department
- Maricopa County Adult Probation Department
- Pima County Adult Probation Department

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.

D. LIMITATIONS

The reader should recognize that this document is a plan and not a set of orders for immediate execution. The sections of this preliminary plan which deal with **Completeness and Accuracy** and **Audit** will require considerably more research and development before procedures can become operative. The Arizona State Justice Planning Agency (ASJPA) encourages local agencies to develop appropriate procedures.

E. EFFECTIVE DATES

Procedures providing for an individual's **Access and Review** of his criminal record, as described in Section IV.E. of this Plan and required by § 20.21(g) of the Regulations, are effective March 15, 1976.

Section IV.A. *Completeness and Accuracy*, Section IV.B. *Limits on Dissemination*, Section IV.C. *Audits and Quality Control*, and Section IV.D. *Security* will be effective March 1, 1978.

F. RESPONSIBILITIES FOR IMPLEMENTATION OF THIS PLAN

As the agency which realizes the heaviest impact of Subpart B of the Regulations, and as the State Central Repository for criminal history record information, the Arizona Department of Public Safety (DPS) is the agency with principal responsibility for the implementation of this Plan. To assist in implementation, the Comprehensive Data System (CDS) Policy Board will consider such policy changes or additions as are necessary within the purview of its authority, and where necessary and desirable seek or assist in obtaining such legislation or Executive Orders as are necessary to accomplish the purposes of this Plan.

G. PENALTIES

Both Arizona law and the Regulations provide sanctions against individuals or agencies who violate law or the Regulations.

Arizona Revised Statute 41-1750D provides that:

Any person who releases or procures the release of information held by the criminal identification section other than as provided by this section, or who uses such information for a purpose other than as provided by this section, is guilty of a misdemeanor.

§ 20.25 of the Regulations provide:

Any agency or individual violating Subpart B of the Regulations shall be subject to a fine not to exceed \$10,000. In addition, LEAA may initiate fund cut-off procedures against recipients of LEAA assistance. Noncompliance with Subpart C may subject an agency to cancellation of information services.

H. THE GENERAL REQUIREMENTS OF THE REGULATIONS

1. Subpart B

The total impact of the Regulations on all affected agencies cannot be accurately assessed at this time. There will certainly be additional costs to be borne by major agencies, and particularly by the Department of Public Safety. As separate subsections of the Regulations become effective, all agencies subject to Subpart B of the Regulations must:

- a. Initiate procedures to assure the completeness and accuracy of criminal history records within their custody. This includes the collection and entry of disposition information when available;
- b. Assure that the most current information is being used by instituting procedures whereby the State Central Repository is queried prior to the dissemination of criminal history information;
- c. Maintain a record of all criminal history record information disseminated in sufficient detail to provide a clear audit trail to include the date of such dissemination, the agency who received it, and the intended use for the information. When an error or omission is revealed, notify all criminal justice agencies known to have received such information;
- d. Assure that personnel employed in the operation of automated or manual record keeping systems are made aware of the substance and intent of the Regulations and receive orientation and training in the compliance therewith;

e. Permit an annual audit of procedures in effect for maintaining the security and privacy of records and controlling the dissemination of criminal history record information;

f. Institute not later than **March 15, 1976**, procedures whereby an individual who believes that criminal history information concerning him is inaccurate, incomplete or maintained in violation of law or regulation, shall, upon satisfactory identification, be entitled to review such information and obtain a copy of it for purposes of challenge or correction. Upon request, an individual whose record has been corrected shall be given the names of all noncriminal justice agencies to whom the data has been given, and all criminal justice recipients shall be notified of the correct information.

2. Agencies subject to Subpart C of the Regulations should comply with Section IX of the Arizona CDS Master Plan. Basically, these are the existing NCIC rules and the DPS Administrative Regulations which have been in effect for the past several years.

SECTION II DEFINITIONS

- A. Definitions Contained in 28 CFR 20**
- B. Arizona Definitions**

Section II DEFINITIONS

For the convenience of the reader, appropriate definitions have been extracted from the Regulations and presented here along with the Arizona interpretations.

A. DEFINITIONS CONTAINED IN 28 CFR 20:

§ 20.3(b) "*Criminal history record information*": 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 to the extent that such information does not indicate involvement of the individual in the criminal justice system.

Interpretation: Any recorded information concerning any person who was arrested, or otherwise entered into the criminal justice process, which record indicates that the criminal justice process that was initiated by that arrest was terminated at any stage of the process, must be regarded as **criminal history record information**. In other words, any record which includes a "disposition" must be considered as a criminal history record. (See "Disposition", below)

§ 20.3(e) "**Disposition**": Information disclosing that criminal proceedings have been concluded, including information disclosing that the police have elected not to refer a matter to a prosecutor or that a prosecutor has elected not to commence criminal proceedings and also disclosing the nature of the termination in the proceedings or information disclosing that proceedings have been indefinitely postponed and disclosing the reason for such postponement. Dispositions shall include, but not be limited to, acquittal, acquittal by reason of insanity, acquittal by reason of mental incompetence, case continued without finding, charge dismissed, charge dismissed due to insanity, charge dismissed due to mental incompetency, charge still pending due to insanity, charge still pending due to mental incompetence, guilty plea, nolle prosequi, no paper, nolo contendere plea, convicted, youthful offender determination, deceased, deferred disposition, dismissed — civil action, found insane, found mentally incompetent, pardoned, probation before conviction, sentence commuted, adjudication withheld, mistrial — defendant discharged, executive clemency, placed on probation, paroled, or released from correctional supervision.

Interpretation: The key words appear to be "that the criminal justice proceedings have been concluded"; not merely that the processing at one stage (arrest, arraignment, prosecution, courts or corrections) has

ended but that the entire action against the individual has terminated. This suggests that record information concerning an individual currently undergoing the criminal justice process is **not** history. Such contemporary information which concerns an active criminal process in Arizona is termed Subject-in-Process information. (See Arizona Definitions, below)

§ 20.3(j) "*Department of Justice criminal history record information system*": The Identification Division and the Computerized Criminal History File systems operated by the Federal Bureau of Investigation.

B. ARIZONA DEFINITIONS

1. "**Subject-in-Process (SIP) Information**" is that information concerning an individual who is currently undergoing the criminal justice process and which does not include a disposition. Subject-in-Process is a cumulative record of events relating to a specific and contemporary criminal justice process. SIP is described in detail in Section III of the Arizona CDS Master Plan.
2. "**State Central Repository**" means the personnel and facility which houses the central file of criminal history within the State of Arizona. Specifically it refers to the Arizona Department of Public Safety-Criminal Identification Section (DPS-CIS).
3. A "**challenge**" is a written contention by an individual that his criminal history record is inaccurate or incomplete; it requires him to give a correct version of his record and explain why he believes his version to be correct.
4. "**Automated**" means the use of electronic computers, including telecommunications networks, microfilm filing and retrieval equipment, as distinguished from performing operations manually.
5. "**Criminal History Record Information User Agreement**" — A contract between the Department of Public Safety-Criminal Identification Section and either a criminal justice agency or a non-criminal justice agency to whom criminal history record information is disseminated by either ACJIS terminals or by other means, that the agency agrees to comply with the rules governing the privacy, confidentiality and dissemination of criminal history record information. The User Agreement qualifies that agency to receive criminal history record information from another agency also qualified to receive criminal history record information.

SECTION III
A BRIEF DESCRIPTION
of the
ARIZONA COMPREHENSIVE DATA SYSTEM
FOR CRIMINAL JUSTICE

- A. Background**
- B. Subsystems of the CDS Program**
- C. Information Contained in Automated Systems**
- D. Manual Record Systems**
- E. Automation — A Gradual Process**
- F. System Management — The Security and Privacy Council and Arizona Rules for Security and Privacy**

Section III

A BRIEF DESCRIPTION OF THE ARIZONA COMPREHENSIVE DATA SYSTEM FOR CRIMINAL JUSTICE

A. BACKGROUND

In order to understand how procedures for implementation of the Regulations will operate, it is important to understand what the criminal justice information system consists of and how it functions. This capsulized description of the Arizona Comprehensive Data System is for the convenience of the reader. The full description is contained in Section III of the CDS Master Plan.

The Arizona Comprehensive Data System for Criminal Justice has two distinct, but closely related, components:

- The statewide Arizona Criminal Justice Information System (ACJIS) network which is an integrated and largely on-line network connecting all of the principal criminal justice agencies in the state and interconnecting to the National Crime Information Center (NCIC) in Washington, D. C., and with the National Law Enforcement Telecommunications System (NLETS); and
- Component Information Systems which are stand-alone information systems designed to serve a particular agency, or groups of agencies within a region, but do not rely on ACJIS as the primary source of information.

ACJIS is conceived as an integrated statewide criminal justice information network serving all agencies of the adult criminal justice system and interfacing with the National Crime Information Center for the exchange of adult criminal record information. ACJIS includes both automated and manual record keeping systems.

From the standpoint of the number of records maintained only a portion of the criminal justice information system is automated. From the standpoint of the number of agencies automated, about 20% are utilizing automated systems. Numerically, the majority of criminal justice agencies in the state maintain manual records. Metropolitan Phoenix and Tucson comprise about 75% of the state's population and about 80% of the reported crime.

B. ACJIS AT A GLANCE

Arizona Criminal Justice Information System (ACJIS) now interconnects 90 criminal justice agencies in Arizona in a single integrated information network. There are 300 remote entry terminals connected to the statewide system. More than 600,000 messages pass through the network each month.

1. Who may join?

Any state, federal or local criminal justice agency may join. This includes police or sheriffs, prosecutors, courts, and adult probation agencies.

2. **What information does ACJIS have access to?**

ACJIS has access to:

- Wanted person files
- Stolen property, including autos and securities
- Stolen weapons
- Outstanding warrants
- Vehicle Registration
- Drivers' Registration (in the near future)
- Computerized Criminal History (for authorized terminals only)
- Subject-in-Process information (in counties that participate in LE-JIS)
- Offender Tracking (by March, 1979)
- Index of persons under supervision of the Department of Corrections

Counties that participate in LAW ENFORCEMENT-JUDICIAL INFORMATION SYSTEM (LE-JIS) have access to the full scope of subject-in-process information from arrest booking through probation.

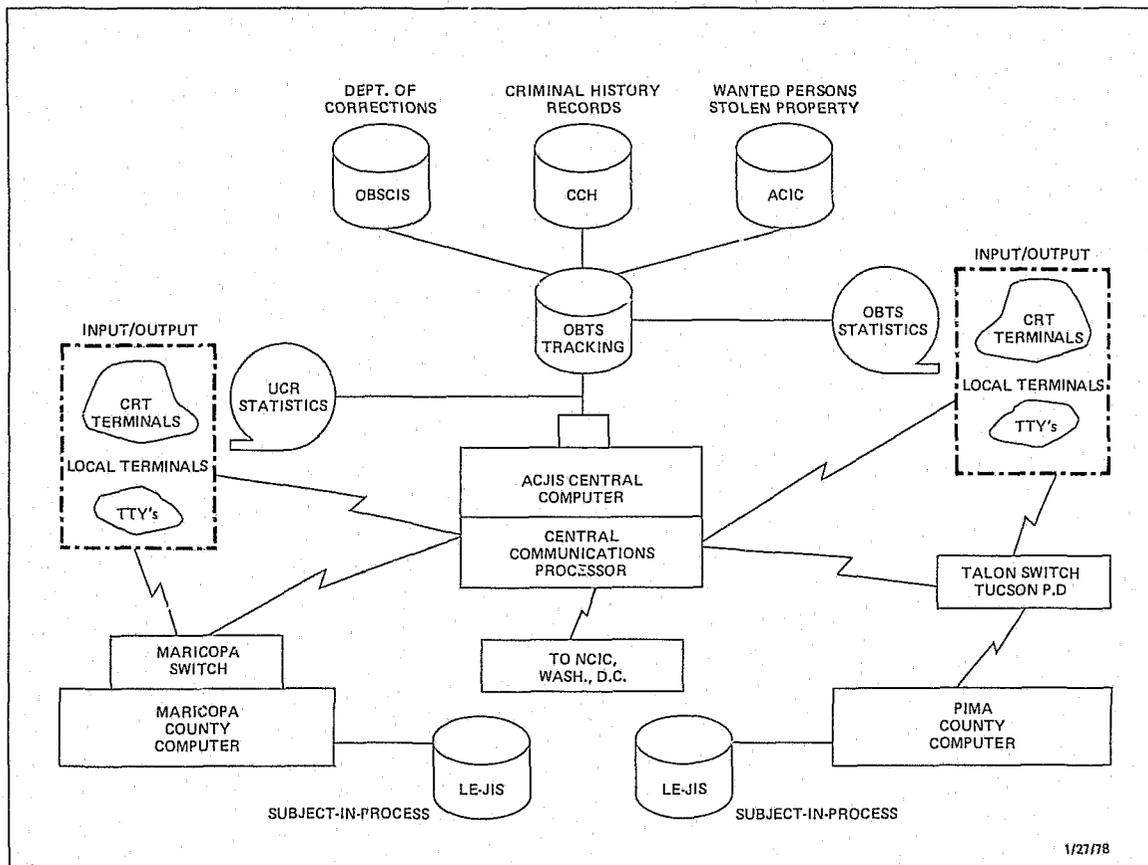
3. **How much delay in response?**

Response to a routine query such as wanted persons or a stolen vehicle is in the neighborhood of 10 seconds. Requests for criminal records take a little longer. If the information requested is not in the Arizona file, the request is automatically routed onward to the National Crime Information Center in Washington, D. C.

4. **Can a terminal in, say Globe, talk to one in Flagstaff?**

Yes, through the National Law Enforcement Telecommunications Service System (NLETS). The ACJIS computer talks directly to the NLETS computer.

ACJIS Information Flow



C. INFORMATION CONTAINED IN AUTOMATED SYSTEMS

1. **There are two distinct types of information which ACJIS, both automated and manual, is concerned with:**

a. **Criminal History Record Information** — which in Arizona is contained within a "dedicated" system at the State Central Repository.

b. **Subject-in-Process (SIP) Information** — which, being contemporaneous, does **not** require totally dedicated computer systems, and which in Pima County is hosted by the Pima County Computer Center, and for Maricopa County is hosted by the Department of Public Safety computer located at the Central Repository. During 1977-1978, the Maricopa County SIP will be transferred to the Maricopa County Information Systems and Services Division (MC-ISSD) in accordance with the Arizona CDS Master Plan.

2. **Information content in subsystems**

The TALON system in Tucson is a message processing system which stores no data. TALON, however, has immediate access to local, state, and national law

enforcement data bases. Tucson local stolen vehicle/license plate information and local wanted persons data is stored in the Tucson City IBM 370-145. TALON also has access to Pima County DPS where the local SIP files are located and to the Central Repository for Criminal History and for Maricopa County SIP information.

The Offender Based State Correctional Information System (OBSCIS) is now in operation, hosted on the DPS computer. OBSCIS interfaces directly with the two county automated SIP systems and thus, will be the Department of Corrections SIP system. OBSCIS concerns itself primarily with correctional information.

Adult Probation Information Systems, being developed jointly in Pima and Maricopa Counties, and hosted on the respective county computers, concern themselves with information necessary for the administration of adult probation and data to support statistical research. As a module of the ACJIS system, the Adult Probation Departments have access to CCH through remote terminals and are covered by Terminal Agency Agreements.

The design of the Adult Probation Information System is such that small counties may gain terminal access. At some future time it is expected that it will become a statewide probation information system.

D. MANUAL RECORD SYSTEMS

Although the automation of record systems is progressing, the vast majority of criminal justice records are maintained by hand. In police agencies record keeping generally follows the pattern set by the FBI's Manual of Police Records. Local police records include complaint reports and investigative records, crime location indices, arrest and identification, and traffic reports. Some, but not all, maintain a master name index. Master Index cards contain a variety of information that may include complaints, victims, arrests, wanted persons, persons injured in vehicle accidents. Index cards often contain fragments of criminal history — usually limited to events occurring within the local jurisdiction.

Larger departments, especially those with an investigative division, maintain jacket files on certain individuals. These jackets usually contain a Rap Sheet or other criminal history along with identification and investigative material. Local jackets on suspects or known criminals are essential to effective police work.

E. AUTOMATION — A GRADUAL PROCESS

In Arizona it is recognized that the complete automation of all criminal justice records will be a gradual process that may take a generation to accomplish. In the meantime, the wisest course of action is to improve manual record keeping methods and to standardize where possible in order to upgrade the quality of law enforcement and criminal justice. Standardized reporting in all segments of the criminal justice system is a major goal. The transition to automated record systems will be greatly eased if manual record systems are upgraded and personnel are accustomed to

working with a high quality record system. To achieve improved manual record keeping systems, a program is underway now to upgrade and standardize record keeping in small police departments.

F. SYSTEM MANAGEMENT — THE SECURITY AND PRIVACY COUNCIL AND ARIZONA RULES FOR SECURITY AND PRIVACY

The Arizona CDS Master Plan, Section V, contains a complete description of the system management structure. Of special significance to this Plan, is the Security and Privacy Council whose mission is to supervise, enforce and adjudicate matters concerning the security and privacy of information. The following is extracted from Section V of the CDS Master Plan:

Security and Privacy Council

A Security and Privacy Council is hereby established which shall be responsible to the Policy Board for the establishment of rules for the security, confidentiality and dissemination of criminal record information as required by applicable law. The Council will consist of seven (7) members, of whom four will represent criminal justice agencies at the state and local level; two lay citizens possessing knowledge and having interest in the criminal justice system and another member skilled and experienced in computer sciences and information technology. At least one of the seven members shall be skilled in the law. Members shall be appointed by the Executive Director, ASJPA, with the concurrence of the CDS Policy Board. A majority of members will be appointed for terms of one year and a minority for terms of two years; thereafter, members will be appointed for two (2) year terms. A member may be reappointed at the expiration of his or her term.

Authority and Responsibilities of the Security and Privacy Council

- Establish by-laws for its own functioning.
- Elect a chairman from among its own membership to serve a term of one year.
- Prepare and submit to the Policy Board for approval, rules, regulations or policies regarding the security, confidentiality and dissemination of criminal record information.
- Adjudicate questions concerning the security, privacy and dissemination of criminal record information and make appropriate recommendations to the Policy Board.
- Evaluate the effectiveness of rules for security, confidentiality and dissemination of criminal record information and make recommendation for changes to the Policy Board.

- Analyze existing legislation pertinent to the security, confidentiality and dissemination of criminal record information, and propose new legislation as appropriate.

Arizona Rules for Security and Privacy

Section IX of the Arizona CDS Master Plan contains the RULES GOVERNING THE PRIVACY, CONFIDENTIALITY AND DISSEMINATION OF CRIMINAL RECORD INFORMATION and for the ADMINISTRATION, MANAGEMENT and SECURITY OF CRIMINAL JUSTICE INFORMATION SYSTEMS in Arizona. These Rules are based on existing Arizona law. They are subject to revision as new regulations and legislation dictates.

SECTION IV OBJECTIVES

- A. Objective #1 — Completeness and Accuracy**
- B. Objective #2 — Limits on Dissemination**
- C. Objective #3 — Audits and Quality Control**
- D. Objective #4 — Security**
- E. Objective #5 — Individual Rights of Access and Review**

Section IV OBJECTIVES

A. OBJECTIVE #1 — COMPLETENESS AND ACCURACY

§ 20.21(a)(1):

To be complete a record maintained at a central State repository which contains information that an individual has been arrested, and which is available for dissemination, must contain information of any dispositions occurring within the State within 90 days after the disposition has occurred. The above shall apply to all arrests occurring subsequent to the effective date of these regulations. 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. 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.

§ 20.21(a)(2):

To be accurate means that no record containing criminal history record information shall contain erroneous information. To accomplish this end, criminal justice agencies shall institute a process of data collection, entry, storage, and systematic audit that will minimize the possibility of recording and storing inaccurate information and, upon finding inaccurate information of a material nature, shall notify all criminal justice agencies known to have received such information.

1. Actions Required by the Regulations

- a. Establish a Central State Repository for criminal history record information;
- b. Dispositions for each finalizing stage (see definition and interpretation of disposition, Section II) of the criminal justice process must be recorded in the criminal record within 90 days after the disposition has occurred;
- c. Procedures must be established to:
 - (1.) Assure that criminal justice agencies query the Central Repository prior to dissemination of criminal history record information to ensure that the most up-to-date data is being used;
 - (2.) Provide that such inquiries of the Central Repository shall be made except in those cases where time is of the essence or the repository is technically incapable of responding within the necessary time period;

(3.) Institute procedures for data collection, entry, storage and systematic audit that will minimize the possibility of recording and storing inaccurate information. Upon finding inaccuracies of a material nature, provide for the notification of all known recipients of the information that inaccuracies were present.

2. Present Situation in Arizona

a. State Central Repository is Operational

(1.) The Criminal Identification Section of the Arizona Department of Public Safety (DPS-CIS) was designated as the Central State Repository by ARS 41-1750 (Attachment B) and ARS 41-2201-6 (Attachment L) and is functioning in that capacity.

DPS-CIS maintains both manual criminal history records and automated CCH records. An on-going CDS project provides for the conversion of manual records to CCH records. At present about 35,000 complete Arizona records are on file in NCIC-CCH and an additional 150,000 partial records are on file in the DPS computer. Forty-seven (47) agencies have entered into Criminal History Record Information User Agreements for access to CCH.

The Department of Public Safety computer center possesses the capacity, the necessary data processing equipment and the telecommunications facilities to provide criminal history record services to all criminal justice agencies in the State. The Comprehensive Data System Master Plan for the State of Arizona, Section III, details the capabilities of the DPS Computer Center.

(2.) Arizona Revised Statutes 41-1750 provides that the Criminal Identification Section of the Department of Public Safety (DPS-CIS) shall:

Procure and maintain records of photographs, descriptions, fingerprints, dispositions and such other information as may be pertinent to all persons who have been arrested for or convicted of a public offense within the state.

The same law also provides that:

The chief officers of law enforcement agencies of the state or its political subdivisions shall provide to the criminal identification section such information concerning crimes and persons arrested for or convicted of public offenses within the state as the chief of the criminal identification section shall deem useful for the study or prevention of crime and for the administration of justice.

and further provides for the issuance of administrative rules and regulations by DPS-CIS for reporting and dissemination of record information. The DPS-CIS Administrative Rules and Regulations of October 4, 1972, set the framework for the reporting of arrests to the DPS-CIS, i.e. the State Central Repository.

(3.) R13-1-04: Information required of all law enforcement agencies of the State of Arizona shall be provided to the Criminal Identification Section of the Department of Public Safety.

A complete set of fingerprints on each initial arrest. Said fingerprints will be imprinted on the appropriate fingerprint form that is provided by the Federal Bureau of Investigation;

For each subsequent arrest, each law enforcement agency of the State of Arizona shall provide to the Criminal Identification Section of the Department of Public Safety one of the following:

- A complete set of fingerprints on the appropriate FBI fingerprint form, and include name, description data, and arrest data; i.e., description of charge, statute number, Arizona Criminal Identification number, and FBI number, if available;
- Department of Public Safety Form 30.60.03 entitled "Additional Arrest Information" completed in full, with Arizona Criminal Identification Section number and the inked impressions of the arrested individual's right four fingers. If the right hand is amputated, imprint the left four fingers and so indicate. In cases where the Criminal Identification Section number is not available, follow the instructions in the paragraph above.
- In all cases where possible on an initial arrest, each law enforcement agency shall provide the Criminal Identification Section of the Department of Public Safety with a photograph of the person arrested, and on the back of said photograph shall inscribe the subject's name, date of birth, description of charge, and statutes violated.

Police agencies are expected to fingerprint and submit cards for all offenses resulting in an incarceration and for all criminal offenses filed in Superior Court. There is no effective method for determining the degree of compliance.

The reverse side of the FBI fingerprint card provides a space for entering arrest disposition. The front side provides a space for final disposition — presumably a court disposition. Rarely are either of these blanks filled in, and there are cogent reasons therefore:

- The FBI card is a method of obtaining a positive identification. The ID function must be performed quickly and therefore, the card often is submitted before an arrest disposition occurs.
- The court disposition follows at some later time, normally on a "Green Sheet", the FBI Final Disposition Form R-84 (Revised 6-29-71). The fingerprint card and a copy of the "Green Sheet" finally join in a record folder. The original "Green Sheet" is forwarded to the FBI.

In Maricopa and Pima Counties, booking is done on-line into the local Subject-in-Process System. Until the Offender Based Tracking and Statistics System (OBTS) is up and running, this entry is of little use to the Central Repository because the Central Repository must rely on manual inputs of the fingerprint cards and final disposition reports. Each agency that provides input data to the local Subject-in-Process System shall institute procedures to assure the completeness and accuracy of information entered into the system. Such procedures will be subject to audit.

b. Reporting of Dispositions

(See definition and interpretation of disposition, Section II)

The key words are "criminal proceedings have been concluded". Any action which terminates the criminal justice process is a disposition. A police decision not to refer charges is a disposition. A prosecutor decision not to commence criminal proceedings terminates a case and is a disposition. Similarly, court actions such as convictions, dismissals, acquittals, and sentences conclude proceedings and are therefore dispositions.

ARS 41-1751 (Attachment C) provides for court disposition reporting in accordance with the rules published by the State Supreme Court. Each submitting agency must accept the responsibility for the accuracy of records submitted.

It is intended that dispositions will be reported to the Central Repository within ninety (90) days after occurrence. Modifications to dispositions will be reported within ninety (90) days after the disturbance of the original sentence or disposition. Disposition reports must provide for the positive identification of an individual through fingerprint identification.

(1.) Rule 37 of the Arizona Rules for Criminal Procedure provides for the manual entry of disposition information.

In every criminal case filed in any court, the final disposition of the case shall be reported to the criminal identification section of the Department of Public Safety. The disposition shall be reported on a

form approved by the Supreme Court. Standard Form XXVII (Attachment D) is provided for reporting dispositions. The completed form shall be sent to the criminal identification section within 10 days of the final disposition.

(2.) Rule 37 of the Arizona Rules for Criminal Procedure provides for the automated entry of disposition information.

In Maricopa and Pima Counties where the events of the judicial process, beginning with arrest booking and continuing through court disposition, are recorded in the Law Enforcement-Judicial Information System (LE-JIS), disposition data will enter the Computerized Criminal History (CCH) file automatically through the Offender Based Tracking and Statistics (OBTS) module. The OBTS module is expected to be operational in March, 1979.

As additional counties subscribe to the LE-JIS network an increasing proportion of dispositions will be entered into CCH automatically.

3. Actions Required Under this Plan

a. Query of the Central Repository Before Dissemination

The Central Repository will maintain accurate and complete records on information submitted by all participants in the criminal justice system. The Regulations provide that procedures shall be established for criminal justice agencies covered under Subpart B of the Regulations and those agencies covered under Subpart C of the Regulations who intend to use the information for secondary dissemination or for dissemination to a non-criminal justice agency to "query the Central Repository prior to dissemination of any criminal history record information to assure that 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".

Agencies who have received information later found to be inaccurate or which has later been amended, and who have contacted the Central Repository by fingerprint card, telephone, teletype, mail or in person will be informed of the inaccuracy or amendment by the Central Repository where the original query was within one (1) year of the change or corrections.

Agencies who have received information later found to be inaccurate or which has later been amended, and who have received criminal history information will be notified by the Central Repository.

b. Promptness of Disposition Reporting

The Central Repository will monitor the receipt of dispositions from all participants in the criminal justice system and institute follow-up procedures

if the time element from arrest to disposition exceeds an estimated due date. Audits of this criterion will be performed in accordance with the procedures set forth under the section entitled "Audits and Quality Control" and will be dependent on legislative and budget constraints.

B. OBJECTIVE #2 — LIMITS ON DISSEMINATION

PART I: Background and General Information

On March 19, 1976, the U. S. Department of Justice, Law Enforcement Assistance Administration issued modifications to those portions of the Security and Privacy Regulations 28 CFR 20 relating to Limitations on Dissemination of Criminal History Record Information § 20.21(f). This section of the Arizona Plan concerns itself with the limitations on the dissemination of criminal history record information as set forth in Subpart B, § 20.21(b) of 28 CFR 20 (Revised).

Note: This plan addresses CHRI which is regulated by Subpart B of the Regulations. As will be seen, some agencies who are subject to Subpart B are also subject to Subpart C of the Regulations by virtue of the fact that they receive CHRI from the NCIC-CCH files of the FBI. In some instances, a conflict may exist between the requirements of Subpart B and Subpart C. **Where such conflict exists, the more stringent rule should be applied.**

1. Applicability of Subpart B

The Regulations concerning dissemination, as contained in Subpart B of the Regulations, apply to all State and local agencies and individuals collecting, storing, or disseminating criminal history record information processed by manual or automated operations **where such collection, storage, or dissemination has been funded in whole or in part with funds made available by the Law Enforcement Assistance Administration subsequent to July 1, 1973, pursuant to Title I of the Act.**

a. The following criminal justice agencies in Arizona have carried out projects the objectives of which were to improve the collection, storage, dissemination or exchange of criminal history record information and, thus, are subject to Subpart B:

- The Arizona Department of Public Safety
- *• The Arizona Department of Corrections
- *• The Phoenix Police Department
- *• The Tucson Police Department
- *• The Maricopa County Sheriff's Department
- *• The Pima County Sheriff's Department
- *• Maricopa County Adult Probation Department
- *• Pima County Adult Probation Department

*These agencies are presently under a Criminal History Record Information User Agreement covering access and dissemination of CHRI.

b. Other Police Agencies

There are a number of smaller police departments in Arizona who have undertaken projects for the overall improvement of manual records keeping and reporting, which made improvement to the storage of fragmentary criminal history or master index records. Likewise, a number of agencies installed terminal equipment providing remote access to ACIC/NCIC for wants, warrants, stolen property or vehicle information. None of these agencies is covered by Subpart B of the Regulations because the terminals do not have access to CHRI. LEAA has stated that §20.20(a) does not apply if the grants were de minimus in amount. None of the records systems grants were directly for the collection, storage, or dissemination of criminal history record information; rather, their goal was general improvement of record-keeping systems and any effect which they might have had on CHRI was peripheral.

Agencies, other than those listed in 1.a. who have entered into User Agreements and thus have access to computerized criminal history (CCH) files in the State Central Repository and through that agency to NCIC-CCH, or are party to a Non-Criminal Justice Agency User Agreement, are covered by Subpart C of the Regulations which are implemented by Section IX of the Arizona CDS Master Plan.

c. Courts

Court records of public judicial proceedings, published court opinions, or public judicial proceedings are exempt from the Regulations. All agencies subject to the Regulations must require that a user agreement exist before sharing CHRI with the courts; the courts are not exempted from the revised regulations, only their official records are exempted.

d. County Attorneys

No county attorney in Arizona has received funds for the collection, storage, or dissemination of criminal history record information. Therefore, none are directly covered by Subpart B of the Regulations or by this Plan. Those county attorneys who are party to Criminal History Record Information User Agreements are subject to Subpart C of the Regulations and Section IX of the Arizona CDS Master Plan.

e. Correctional Agencies — Adult Probation Departments

Adult probation departments may deal with both conviction and non-conviction information. As indicated in 1.a., both Maricopa and Pima County Adult Probation Departments are covered by Subpart B of the Regulations. Other county adult probation departments who are party to

Criminal History Record Information User Agreements or Non-Criminal Justice Agency User Agreements are subject to Subpart C of the Regulations and Section IX of the Arizona CDS Master Plan.

2. **Applicability of Subpart C**

§ 20.30 "The provisions of this Subpart of the Regulations apply to any Department of Justice criminal history record information system that serves criminal justice agencies in two or more states and to Federal, state and local criminal justice agencies to the **extent** that they utilize the services of the Department of Justice criminal history record information systems. These regulations are applicable to both **manual and automated systems.**"

An agency that receives an FBI "Rap" sheet on an individual is subject to Subpart C of the Regulations to the extent of the information contained in that "Rap" sheet.

3. **Conviction Data versus Non-Conviction Data**

The revised Regulations draw a distinction between the dissemination of "conviction information" and "non-conviction information".

§ 20.3(k) "**Non-conviction data**" means arrest information without disposition if an interval of one year has elapsed from the date of arrest and no active prosecution of the charge is pending; or information disclosing that the police have elected not to refer a matter to a prosecutor, or that a prosecutor has elected not to commence criminal proceedings, or that proceedings have been indefinitely postponed, as well as all acquittals and all dismissals.

Note: The reader's attention is called to the definitions of "criminal history record information" and "disposition" given in Section II.A. of this Plan.

Limits on dissemination of conviction and non-conviction information are found in § 20.20(c) and (b) and § 20.21(b) of the Regulations.

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 non-criminal justice recipients, to the full extent that such dissemination is not prohibited by law. Any state or local law or order limiting dissemination of such data would not be affected by the Regulations; as for example ARS 41-1750 which limits the extent to which DPS-CIS may disseminate conviction information.

The only dissemination limits imposed by the Regulations relate to "non-conviction data", defined by § 20.3(k) to include information disclosing that the police have elected not to refer a matter for prosecution, a prosecutor has elected not to commence criminal proceedings, proceedings have been indefinitely postponed, all dismissals, all acquittals, and arrest record 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 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 non-conviction data until the charges are ultimately dismissed. Where prosecution has been officially deferred to divert the defendant to a treatment alternative program, such a deferral is a disposition and should be entered on record. 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.

The operational impact of the distinction between conviction and non-conviction information, so far as the rules are concerned, is that agencies in disseminating conviction information need not require that the recipient be party to a user agreement. Further, **it is permissible to disseminate to anyone the information that an individual has no convictions. But the dissemination must be clearly phrased so it will not imply that the individual has any other form of criminal record.** The form currently in use by CIS states as follows:

"A search of the Department of Public Safety's Arizona Criminal History file reveals that there is no record of any misdemeanor or felony conviction on the above named person."

This statement meets the requirements of the Regulations. (See Attachment E)

4. **Criminal History Record Information Not Covered by Subpart B**

§ 20.20(b) provides as follows:

The regulations in this subpart shall not apply to criminal history record information contained in: (1) Posters, announcements, or lists for identifying or apprehending fugitives or wanted persons; (2) Original records of entry such as police blotters maintained by criminal justice agencies, compiled chronologically and required by law or long standing custom to be made public, if such records are organized on a chronological basis; (3) Court records of public judicial proceedings; (4) Published court or administrative opinions or public judicial, administrative or legislative proceedings; (5) Records of traffic offenses maintained by State departments of transportation, motor vehicles or the

equivalent therefore for the purposes of regulating the issuance, suspension, or revocation, or renewal of driver's, pilot's or other operator's licenses; (6) announcements of executive clemency.

a. Subject-in-Process Information

§ 20.20(c) provides as follows:

Nothing in these Regulations prevents a criminal justice agency from disclosing to the public, criminal history record information related to the offense for which an individual is currently within the criminal justice system.

The subject-in-process systems (known as the Law Enforcement-Judicial Information Systems, LE-JIS) deal strictly with contemporary information and are not subject to the rules relating to Dissemination or Security. LEAA letter of October 22, 1976, states in part:

... it is concluded that Section 20.20(c) is more limited in its scope, exempting subject-in-process systems from the "Dissemination" requirement and by implication the "Security" requirement, only.

However, in the interests of the individual and to avoid the possibility of civil liabilities, subject-in-process records should be complete and accurate and available for access and review.

b. Release to News Media and Others

§ 20.20(c) provides as follows:

A criminal justice agency is not prohibited from confirming prior criminal history record information to members of the news media or any other person upon specific inquiry as to whether a named individual was arrested, detained, indicted, or whether an information or other formal charge was filed, **on a specified date**, if the arrest record information or criminal record information is based on data excluded by paragraph § 20.20(b).

In Arizona, such disclosures are permitted because the information may also be found on original records of entry open to public inspection.

c. Passports, Visas, Foreign Travel

The Regulations permit the dissemination of criminal history record information for purposes of international travel, such as issuing visas and granting of citizenship. This applies to **both** conviction and non-conviction information.

d. Radio Communications

The revised regulations do not restrict the dissemination of CHRI by radio communication to patrol cars or other mobile units.

5. **Arizona Law and Local Ordinances**

a. Law Relating to DPS-CIS

ARS 41-1750 prescribes the duties of the Criminal Identification Section of the Department of Public Safety (State Central Repository) for the collection, storage and dissemination of criminal record information. **Except for Sections C and G, ARS 41-1750 applies only to CIS, not to other agencies.**

ARS 41-1750-F permits the chief of the Criminal Identification Section to issue rules, subject to the approval of the director, for the dissemination of conviction information to those agencies of state or local government who have issued appropriate rules, regulations or ordinances, as provided under 41-1750-G, requiring background investigations of prospective employees or licensees. Further, ARS 41-1750 does not specifically prohibit the secondary dissemination of CIS information for purposes of criminal justice:

41-1750F Provides that the chief of the criminal identification section subject to the approval of the director, shall make and issue rules and regulations relating to the procurement and dissemination of information, in the manner prescribed by law.

41-1750-G. All non-law enforcement agencies of the state or its political subdivisions may establish by rule, regulation or ordinance the need for fingerprint or background investigations for purposes of employment or licensing and may, thereafter, utilize the criminal identification section of the department of public safety in accordance with Subsection F.

41-1750B.5. Provide information from its records to law enforcement agencies of the state or its political subdivisions upon request by the chief officer of such agency or his authorized representative. Such information shall be used only for purposes of law enforcement.

41-1750B.6. Provide information from its records to courts, prosecutors or correctional agencies of the state or its political sub-divisions upon request by the chief officer of such agency or his authorized representative. Such information shall be used only for purposes of the criminal justice system.

Under Sections B.7 and B.8, non-criminal justice recipients of CIS may use the information for evaluating prospective employees and licensees:

41-1750B.7. Provide information from its records relating to convictions for public offenses to non-law enforcement agencies of the state or its political subdivisions upon request by the chief officer of such agency or his authorized representative, for the purpose of evaluating the fitness of prospective employees of such agency. Such information shall be used only for the purpose of such evaluation.

41-1750B.8. Provide information from its records relating to convictions for public offenses to licensing and regulatory agencies of the state or its political subdivisions upon request by the chief officer of such agency or his authorized representative, for the purpose of evaluating the fitness of prospective licensees. Such information shall be used only for the purpose of such evaluation.

b. Law Relating to the Arizona Department of Corrections

ARS 31-221 requires the Department of Corrections to maintain a master record file on each person committed to it and specifies the minimum content of that file. That law also makes the DOC files confidential and strictly limits access to certain authorized personnel, and requires that a record be kept of personnel of other correctional or law enforcement agencies who view them. ARS 31-221 gives the Director of DOC rule making authority for access to files.

6. **Dissemination Standards**

a. Query of Central Repository

The Regulations require criminal justice agencies to query the State Central Repository before disseminating CHRI. **Query is not required when agencies use their own information internally.** This rule applies to all criminal justice agencies who are party to a Criminal History Record Information User Agreement with the Criminal Identification Section to receive information. Before disseminating CHRI outside the agency, either the disseminating agency or the receiving agency should query the State Central Repository for the most recent record information.

Query of the Central Repository is not required for:

(1.) The furnishing of information for the purpose of processing a charge through the criminal justice system when it is clear under the circumstances that no disposition had occurred and the information which is furnished relates only to the charge in process;

(2.) Verbal discussion of an individual's criminal record among representatives of criminal justice agencies for purposes of the administration of criminal justice where there is no written or printed exchange of CHRI, up-dating of an agency's CHRI files, or creation of a new file based on the discussions.

These rules will be written into the Criminal History Record Information User Agreement.

b. Audit Trail

The Regulations require that all agencies disseminating CHRI subject to Subpart B of the Regulations shall record, at a minimum for each transaction, **the names of all persons and/or agencies to whom information is disseminated, the date upon which such information is disseminated, and the purpose for which the request for information was made.** In accordance with § 20.21(e) in manual systems, this requirement can be satisfied by attaching a dissemination record or an individual receipt form to each case file.

This plan requires **case** dissemination records whenever information is disseminated **outside** of the criminal justice system. When information is disseminated **among** criminal justice agencies, logs or receipts are not required. (The term log means any written record of a transaction which serves to establish an audit trail. A log may consist of a formal log book; amount to a notation in an existing record; or be in the form of a receipt. The automated record of queries against a computer file is also termed a log.)

Four exceptions to the recording of dissemination of information are:

- The furnishing of information for the purpose of processing a charge(s) through the criminal justice system when it is clear under the circumstances that no disposition has occurred and the information which is furnished relates only to the charge(s) in process;
- Verbal discussion of an individual's criminal record among representatives of criminal justice agencies for purposes of the administration of criminal justice where there is no written or printed exchange of CHRI, up-dating of an agency's CHRI files, or creation of a new file based on the discussions;
- The automated exchange of information between a repository and those agencies to which it provides information under criminal justice user's agreements;
- The automated exchange of information among criminal justice agencies which participate in an automated multiple-agency information system with a common data base such as CAD/CAPRI.

In regard to the first two exceptions, LEAA has already singled out these transactions as special situations.

In regard to the last two exceptions, Arizona has weighed the cost of maintaining dissemination records against its usefulness and concluded that other measures exist which protect privacy just as well without the added burden of case dissemination records. Arizona will implement these alternative measures as described in the following paragraphs:

First, the case dissemination record is viewed as a technique for promoting accuracy. According to the Revised Instructions, "Logging is required for the support of the audit process and also as a means of correcting erroneous information." But the Central Repository query rule already insures that agencies are more likely to receive information which is accurate and up-to-date, and it greatly increases the number of record disseminations which the Central Repository must record.

In an automated system **none** of the alternative methods of "logging" dissemination are attractive. Valuable storage space has to be set aside on **all** records in order to record all potential disseminations even though, as statistics show, only about 15% of all CIS records are ever accessed. The DPS Computer Center maintains a magnetic tape query log of the CCH file which is useful for auditing, but the tracking of individual records recorded on tape is a time consuming and costly operation.

In the closed regional system, the audit trail requirement discourages multi-agency cooperation by requiring an act which agencies would not have to perform if they had left their records in internal systems. Arizona is moving toward automated region-wide, closed information systems in the metropolitan areas. Such systems as the Phoenix Computer Aided Police Record Index (CAPRI) will eventually link several local police agencies into a common system using a common data base.

The LEAA Privacy and Security Planning Instructions state that the log should be used as a basis for notifying agencies which may have received erroneous CHRI. Under this Arizona Plan, agencies subject to the logging exception must agree that **whenever an error is found on any of their records**, they will notify **all** criminal justice agencies on their authorized dissemination list. Thus, the same objective is reached without the log (which only covers transactions within the last year anyway).

Second, one may assume that the record of case disseminations will uncover disseminations improperly made because of mistake or carelessness. This is true in the case of non-criminal justice dissemination, which dissemination is more restrictive. Although not required by this Plan (See exceptions to logging, Section IV, B.6.b.), the Criminal Identification Section has continued to log CCH inquiries by remote terminals in order to provide an audit trail of dissemination to various agencies. This procedure also permits the monitoring of excessive terminal activity.

The external dissemination of non-conviction CHRI is a totally different matter; whenever non-conviction CHRI is transferred to an individual or agency **outside** the criminal justice community, appropriate records of who, what, when, and why must be maintained. (See AUDIT, Section IV.C. of this Plan).

c. Criminal History Record "Use" Codes

The National Law Enforcement Telecommunications Systems has adopted a set of "use" codes to be included in the audit trails of the dissemination of CHRI. All NLETS subscribers will be required to utilize the NLETS codes in CHRI queries or responses. Although not required, these codes are available for use by any agency for the purpose of indicating the end use of CHRI which is disseminated:

Code	Meaning
C	Criminal Justice Purposes
E	Authorized Licensing and/or Employment Purposes
R	Information Provided to Individuals Who Wish to Review and/or Challenge Their Criminal History Record

d. Notices to Receiving Agencies

Privacy and Security Planning Instructions published on June 30, 1975, stated that "written notice to receiving agencies is an essential procedure ... Each disseminating agency subject to these regulations has the burden of giving notice of the requirements of the regulations". Since this section has been omitted from the revised planning instructions, this plan assumes notices are no longer required.

e. Special Dissemination Rules

The revised regulations create special dissemination rules which, for example, limit secondary dissemination when information is transferred outside of criminal justice, and provide that the existence of CHRI may be neither confirmed nor denied **except** to an individual or agency who would otherwise have access to that record. All of these requirements will be written into appropriate criminal justice and non-criminal justice user agreements to assure that recipients are:

- Aware of the limits on the use of non-conviction CHRI and the penalties attached to its misuse;
- Prepared to enforce appropriate measures to insure the security and confidentiality of CHRI.

f. User Agreements

The term User Agreements deserves explanation. Basically, a user agreement is a contract between an agency (either criminal justice or non-criminal justice) and the State Central Repository, in this case DPS-CIS, which describes the conditions under which an agency may receive CHRI and the manner in which such information must be treated. All user agreements must provide assurances that the recipient agency is:

- Eligible to receive non-conviction CHRI;
- Aware of the limits on the use of non-conviction CHRI and the penalties attached to its misuse;
- Prepared to enforce appropriate measures to insure the security and confidentiality of CHRI.

In this Plan, reference is made to the need for awareness, on the part of a disseminating agency, of the existence of a user agreement before CHRI may be disseminated to another agency. In order to receive CHRI from any agency, an agency need only be party to a **single user agreement. It will be the responsibility of the State Central Repository to publish and keep current a list of agencies who are party to user agreements.**

7. Dissemination Outline for Agencies Subject to the Regulations

Requirements marked with a double asterisk (**) apply to all criminal justice agencies in the state.

- a. Is the information on
- a pending case?
 - requested by a chronological inquiry?
 - sought for purposes of international travel?

If so, the information may be freely shared.

(1.) A pending case is one where the defendant is still in the criminal justice system with the following exceptions:

- the case is more than one year old and no judicial disposition is recorded and it is not scheduled for a criminal proceeding and the defendant is not a fugitive.
- the disposition has been indefinitely postponed except where prosecution has been deferred or postponed to divert the defendant into an alternative treatment program.

(2.) A chronological inquiry is an inquiry such as the following: "Was John Jones arrested on June 17, 1943?"

(3.) Agencies may follow existing practices regarding the dissemination of CHRI for passports, visas, or tourist passes.

****b.** If the information is none of the above, is the information from the Criminal Identification Section?

(1.) CIS information may only be shared with other criminal justice agencies.

(2.) Verify that the recipient agency has signed a user's agreement.

(3.) Query CIS prior to dissemination unless one of the exceptions applies.

(4.) Log the dissemination unless one of the exceptions applies.

c. If it is not information from CIS, is it information which indicates a conviction?

(1.) Conviction information may be shared with anyone.

******(2.) Query CIS prior to dissemination unless one of the exceptions applies.

(3.) Log the dissemination unless one of the exceptions applies.

d. If the information is not conviction information, is the requestor a criminal justice agency?

(1.) Foreign criminal justice agencies may receive CHRI under § 20.21(b)(3). [See paragraph g.(1.) of the Regulations]

******(2.) Verify that the recipient agency has signed a user's agreement.

*****(3.) Query CIS prior to dissemination unless one of the exceptions applies.

(4.) Log the dissemination unless one of the exceptions applies.

e. If the requestor is not a criminal justice agency, has the Attorney General of Arizona and/or the U.S. Attorney General authorized the dissemination of criminal justice information to the requestor?

(1.) Attorney General authorization is evidence of legislative authority (statute, executive order, or ordinance) to receive criminal justice information under Rules 5 and 6 of the Department of Public Safety, Criminal Identification Section, Administrative Rules and Regulations.

(2.) Verify that the recipient agency has signed an appropriate user's agreement.

******(3.) Query CIS prior to dissemination unless one of the exceptions applies.

(4.) Log the dissemination unless one of the exceptions applies.

f. If the requestor is not authorized by the Attorney General, is the requestor authorized by court order, rule, or decision?

(1.) Verify that the recipient has signed an appropriate user's agreement.

** (2.) Query CIS prior to dissemination unless one of the exceptions applies.

(3.) Log the dissemination unless one of the exceptions applies.

g. If the requestor is not authorized by court order, rule, or decision, can information be shared pursuant to § 20.21(b)(3) (services required for the administration of criminal justice) or § 20.21(b)(4) (research, evaluative, or statistical activities)?

(1.) Foreign criminal justice agencies may receive CHRI under § 20.21(b)(3).

(2.) Follow the procedures which 28 CFR 20, § 20.21(b)(3) and (4) describe.

h. If the information may not be shared pursuant to § 20.21(b)(3) or (4), tell the requestor: **The information requested either does not exist or may not be shared.**

8. Juvenile History Data

When a juvenile is tried as an adult, the juvenile criminal history record data is treated as adult CHRI.

When a juvenile is before the juvenile court on a delinquency petition, the revised regulations do not permit the dissemination of this information outside of criminal justice unless dissemination is authorized by "statute, court order, rule or court decision". In Arizona, the authority for such dissemination is contained in a court decision, *Parsons v 504 P2d 1272* (1973) which held that juvenile court orders of disposition are matters of public record.

Juvenile record information is not contained in the Arizona Criminal Justice Information System nor is it filed with the State Central Repository.

PART II: Arizona Plan for Action

It is planned that the following policies, relating to the dissemination of conviction and non-conviction criminal history record information, will be implemented by appropriate agencies prior to December 31, 1977:

1. DPS-CIS

a. Under the authority of 41-1750F, issue rules for the dissemination of non-conviction information to non-criminal justice agencies of the state or its political subdivisions who establish that the appropriate rules, regulations, or ordinances are extant;

b. Develop suitable user agreements to bind non-criminal justice users of

non-conviction information to the requirements for control of that information;

c. To permit disseminating agencies to be certain that a potential recipient is an agency permitted to receive information, establish a procedure which will assure that a list of all non-criminal justice agencies who are party to a user agreement, a Criminal History Record Information User Agreement or a Non-Criminal Justice Agency User Agreement is maintained and distributed to all criminal justice agencies in the state on a timely basis;

d. Establish records to assure an audit trail of CHRI information disseminated to authorized non-criminal justice persons or agencies.

2. Other Criminal Justice Agencies Subject to Subpart B of the Regulations

a. Establish procedures for the control of the dissemination of non-conviction information to non-criminal justice persons and users. This includes the encouragement of council or board of supervisors for enactment of appropriate rules or ordinances;

b. Establish procedures requiring that non-criminal justice agencies provide evidence of their authority to obtain access to non-conviction information prior to gaining access;

c. Provide appropriate user agreements for non-criminal justice agencies who have access to non-conviction information;

d. Establish record-keeping procedures sufficient to provide a clear audit trail for either conviction or non-conviction information disseminated to non-criminal justice agencies or individuals;

e. Establish procedures for querying the State Central Repository prior to the dissemination of criminal history record information.

C. OBJECTIVE #3 — AUDITS AND QUALITY CONTROL

§ 20.21(e) **Audit.** 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. Such records shall include, but are not limited to, the names of all persons or agencies to whom information is disseminated and the date upon which such information is disseminated.

Inherent in Section 524(b) of the Omnibus Crime Control and Safe Streets Act is the requirement that those criminal justice agencies covered by Subpart B of the Regulations devise some method for monitoring compliance with restrictions set out in the legislation. The Regulations address this problem by requiring that appropriate accounting be kept of the dissemination of criminal history record information, and

that the State conduct an annual audit of a representative sample of State and local criminal justice agencies covered by Subpart B of the Regulations to verify adherence to the Regulations. Subpart C of the Regulations does not address the subject of audit. The criteria for audit will be established by the CDS Security and Privacy Council.

The Regulations call for two different forms of auditing:

- The **systemic audit** is required for the Central Repository as a means of guaranteeing the completeness and accuracy of the records. This audit is actually a quality control mechanism which will be part of the systems and procedures designed for the criminal history repository.
- The **annual audit** is an examination, by the Central Repository, of the extent to which statewide users are complying with the Regulations. The Central Repository may be audited by the FBI, the NCIC Advisory Policy Board, as well as by an outside agency appointed by the CDS Policy Board.

1. **Systemic Audit**

This systemic audit refers to the combination of systems and procedures employed both to ensure completeness of records and to verify accuracy. Procedures, dealing with checking on completeness, assume that the disposition reporting system described previously will provide an adequate means for monitoring the submission of disposition data.

The Central Repository will institute a delinquent disposition report monitoring system. This system will be based on estimating expected arrival dates for final dispositions, which reflect anticipated processing time for each type of criminal offense. If an accrued disposition is not received by the estimated due date, appropriate follow-up must be started to obtain the required disposition information.

Procedures will be established in automated systems to automatically withhold the dissemination of information covered under the one-year rule to agencies having terminal access to the system which are prohibited from receiving the information covered.

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

a. **Audit Trail**

An audit trail will be established which will allow for the tracing of specific data elements back to the source document. This audit trail will encompass all participating agencies in the criminal history records system

covered by Subpart B of the Regulations and will reflect specific agencies who have made entries on source documents or input formats supporting the system.

b. Dissemination Audit Trail

The audit trail covering input to the system will 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. An audit trail will be required for the support of the audit process; and as a means of correcting the dissemination of incomplete or erroneous information.

c. Audit of Subject-in-Process Systems

Agencies who enter information into a Subject-in-Process system will be audited annually to assure that procedures are in effect to assure the completeness and accuracy of information so entered. Those agencies will also be subject to annual audit to assure that procedures are in effect to permit an individual to gain access to his record for purposes of review and/or challenge.

All Arizona criminal justice agencies covered under Subpart B of the Regulations will prepare a form suitable to their agency for use as a receipt for all criminal history information disseminated to non-criminal justice agencies. At its discretion, an agency may utilize a log book procedure. All agencies which are covered under Subpart C of the Regulations and which use the criminal history record information received from NCIC or CCH as secondary dissemination, or who disseminate it to a non-criminal justice agency, are also required to keep an audit trail. Secondary dissemination is defined as the transfer of CHRI to a third party. The receipts will bear notation of date, agency, individual to whom the record was released and the intended purpose. This receipt must be kept for a minimum of two (2) years and be readily accessible for audit. This applies to all agencies covered under either Subpart B or Subpart C of the Regulations.

The logging of CCH transmissions directly from the computer file will be performed by suitable software and hardware.

Attachment F shows an example of a form that is adequate for recording dissemination of information from any agency where an audit must be established. This receipt can be stored chronologically or alphabetically.

2. Annual Audit

Annual audits of a representative sample of State and local criminal justice agencies chosen on a random basis will be conducted under the direction and control of the CDS Policy Board, as recommended by the Security and Privacy Council, to verify adherence to the Regulations. Procedures will be developed for annual audits which will outline the specific sampling approach to be taken to include the number, type, location, size of agency to be audited.

Audit of the State Central Repository will be performed by another agency so designated by the CDS Policy Board.

Sampling procedures will be established for the examination of specific records at the Central Repository level to be traced through internal update procedures back through filed input processing to terminate at the source document. Areas to be reviewed will include, but not be limited to, record accuracy, completeness, review of the effectiveness of systemic audit procedures, and examination of the evidence of dissemination limitations, security provisions, and the individual's right of access. The audit plan will address audits of both manual and computerized systems.

Adequate documents and audit trails must be maintained by the agencies to support the annual audit. This documentation will include, but not be limited to, maintaining source documents (at the point of data entry) from which criminal history information stored at the Central Repository is derived.

3. Situation in Arizona

In order to determine how law enforcement agencies around the State maintain records of released information, a survey was conducted of ten agencies of various size. It was determined that about ninety percent (90%) of the departments are maintaining some type of basic record for information transferred to other agencies. The majority of the agencies are using a simple receipt system.

Concerning information generated internally, the method used for recording dissemination varies from agency to agency. Most agencies are using some type of request/receipt slip. These are usually filled out each time a request for information is received, either in person or by telephone. The storage of these request/receipt slips ranges from in-jacket storage to chronological filing or both. In some cases two copies are required, one for jacket filing, the other for chronological filing.

Because there has never been a set standard established within the criminal justice system for the filing of receipt documents, the time of retention varies from immediate destruction to permanent filing. Most agencies retained receipts from 6 months to 1 year.

4. Actions Required

Section IX of the CDS Master Plan must be revised to require the agencies covered under Subpart C of the Regulations, who are engaged in secondary dissemination of criminal history information or who disseminate to non-criminal justice agencies, to keep an audit trail of what they have released and to whom. The Security and Privacy Council will be responsible for making recommendations to the CDS Policy Board for:

- a. Systemic Audit Procedures

- b. Annual Audit Procedures
- c. Audit Trail Procedures

(1.) Those agencies covered under Subpart B must maintain an audit trail of all dissemination of criminal history record information to a non-criminal justice agency.

(2.) Those agencies covered under Subpart C must maintain an audit trail for all secondary dissemination or dissemination to a non-criminal justice agency.

D. OBJECTIVE #4 — SECURITY

§ 20.21(f) **Security.** Where criminal history record information is collected, stored, or disseminated, each State shall insure that the following requirements are satisfied by security standards established by State legislation, or in the absence of such legislation, by regulations approved or issued by the Governor of the State.

(1) Where computerized data processing is employed, effective and technologically advanced software and hardware designs are instituted to prevent unauthorized access to such information.

(2) Access to criminal history record information system facilities, systems operating environments, data file contents whether while in use or when stored in a media library, and system documentation is restricted to authorized organizations and personnel.

(3)(A) Computer operations, whether dedicated or shared, which support criminal justice information systems, operate in accordance with procedures developed or approved by the participating criminal justice agencies that assure that:

(i) Criminal history record information is stored by the computer in such a manner that it cannot be modified, destroyed, accessed, changed, purged, or overlaid in any fashion by non-criminal justice terminals.

(ii) Operation programs are used that will prohibit inquiry, record updates, or destruction of records, from any terminal other than criminal justice system terminals which are so designated.

(iii) The destruction of records is limited to designated terminals under the direct control of the criminal justice agency responsible for creating or storing the criminal history record information.

(iv) Operational programs are used to detect and store for the output of designated criminal justice agency employees all unauthorized attempts to penetrate any criminal history record information system, program or file.

(v) The programs specified in (ii) and (iv) of this subsection are known only to the criminal justice agency employees responsible for criminal history record information system control or individuals and agencies pursuant to a specific agreement with the criminal justice agency to provide such programs and the program(s) are kept continuously under maximum security conditions.

(vi) Procedures are instituted to assure that an individual or agency authorized direct access is responsible for the physical security of criminal history record information under its control or in its custody and the protection of such information from unauthorized access, disclosure or dissemination.

(vii) Procedures are instituted to protect any central repository of criminal history record information from unauthorized access, theft, sabotage, fire, flood, wind, or other natural or manmade disasters.

(B) A criminal justice agency shall have the right to audit, monitor and inspect procedures established above.

(4) The criminal justice agency will:

(A) Screen and have the right to reject for employment, based on good cause, all personnel to be authorized to have direct access to criminal history record information.

(B) Have the right to initiate or cause to be initiated administrative action leading to the transfer or removal of personnel authorized to have direct access to such information where such personnel violate the provisions of these regulations or other security requirements established for the collection, storage, or dissemination of criminal history record information.

(C) Institute procedures, where computer processing is not utilized, to assure that an individual or agency authorized direct access is responsible for (i) the physical security of criminal history record information under its control or in its custody and (ii) the protection of such information from unauthorized access, disclosure, or dissemination.

(D) Institute procedures, where computer processing is not utilized, to protect any central repository of criminal history record information from unauthorized access, theft, sabotage, fire, flood, wind, or other natural or manmade disasters.

(E) Provide that direct access to criminal history record information shall be available only to authorized officers or

employees of a criminal justice agency, and, as necessary, other authorized personnel essential to the proper operation of the criminal history record information system.

(5) Each employee working with or having access to criminal history record information shall be made familiar with the substance and intent of these regulations.

1. Actions Required by the Regulations

The Federal Regulations require that adequate security standards be established wherever criminal history record information is collected, stored, or disseminated to:

- a. Present unauthorized access to the criminal history record information files (whether computerized or manual);
- b. Prevent unauthorized access to the facilities;
- c. Insure that criminal history record information cannot be modified, destroyed, accessed, etc. by non-criminal justice terminals;
- d. Prohibit inquiries and updates by other than criminal justice terminals;
- e. Prohibit unauthorized destruction of records (whether computerized or manual);
- f. Record unauthorized attempts to penetrate the CHRI files;
- g. Guarantee security sensitive segments of the operating system are open only to authorized personnel;
- h. Protect the Central Repository from unauthorized access, theft, fire, etc.
- i. Screen and select personnel to be authorized to have access to the CHRI files or facilities.

2. Situation in Arizona under this Plan

It is policy as established in Section VIII of the Arizona CDS Master Plan that the Arizona Computerized Criminal History Information System utilize the necessary hardware, software, management control, personnel selection, and physical security procedures to insure that all criminal history information will be protected against unauthorized access, use and/or dissemination.

a. Hardware

The Regulations require that "effective and technologically advanced... hardware designs are instituted to prevent unauthorized access" to CHRI [§ 20.21(f)(1)]. Arizona has already adopted such designs.

The Arizona CDS Master Plan sets forth the concept that information pertaining to the offense for which an individual is currently within the

criminal justice system is classed as Subject-in-Process data which will be housed at a local and/or regional level. That information concerning the criminal justice transaction which is historical in nature and which is defined as criminal history information, will be stored on a dedicated computer system at the State Central Repository, the Department of Public Safety in Phoenix, Arizona.

The Department of Public Safety, Criminal Identification Section (DPS-CIS) performs the function of State Central Repository. CIS collects, stores and maintains criminal record information as required by applicable State law. CIS utilizes the facilities of the DPS-Data Processing Section (DPS-DP) for the collection, storage and maintenance of computerized criminal history (CCH). The DPS-DP Section computer is dedicated exclusively to criminal justice purposes; it links directly to the NCIC computer via a front end message processing computer.

The distinction between local Subject-in-Process data and statewide criminal history information is relevant to the implementation of security measures. While the former systems are not exempt from the revised regulations, their security does not require all of the exceptional measures stated in § 20.21(f). All of the information in these systems may be freely disseminated to the public under § 20.20(c); where unauthorized access results in record alteration or destruction, the same information may be found stored in manual files and often in the manual files of more than one agency. The security standards already adopted by the criminal justice and electronic data processing agencies which operate these systems will be adequate to satisfy the security objectives contained in the Regulations.

On the other hand, this plan requires that local message processing computers and terminals which provide access to the Central Repository's criminal history information must fully meet the applicable requirements of § 20.21(f).

All computerized criminal justice transactions, be they Subject-in-Process information or criminal history stored in the Central Repository, can be accessed by criminal justice agencies through computer terminals which are connected to a communications processor through the data telecommunications system. The communications processors serve as access and switching systems to the stored data. The switching computers are thus able to screen all attempts to access the Subject-in-Process data stored at a local and/or regional level. All inquiries to the Computerized Criminal History (CCH) information stored at the Central Repository are screened to permit dissemination only to those terminals authorized to receive it. The switching computers in Pima County, part of the TALON System, which serve Southern Arizona, are located in and under the direct control of the Tucson Police Department. The switching computers for Maricopa County agencies will be located in the Maricopa County Information Systems and Services Division (ISSD). An appropriate interagency agreement will be

effected between ISSD and the Sheriff's Department to assure compliance with the Regulations. The City of Phoenix criminal justice agencies are to be served by a switching computer located in and under the control of the Phoenix Police Department as part of the CAD-CAPRI System. The concept of switching computers provides both a security lock and a message switch for the agencies they serve.

On the state level, the Central Repository utilizes a front-end message and processing computer to screen all attempts from all terminals and switching computers to access the criminal history data base. Through a combination of hardware and software, only those terminals authorized to have access to the Computerized Criminal History file are allowed to retrieve information and only specific agencies are allowed to update the information. An access log of queries against CCH is maintained off-line on tape.

The storage devices which are utilized for the storage of Subject-in-Process information in the Arizona Criminal Justice Information System are on-line storage units. These units will, in all cases, be totally dedicated to criminal justice information. The terminals utilized in the criminal justice agencies which are authorized access to criminal justice information are also fully dedicated to criminal justice purposes.

All criminal justice agencies within the State of Arizona which have, or will have, the capability to access the criminal history record information files must enter into a Criminal History Record Information User Agreement with the Department of Public Safety. In addition to this procedural contract, a Terminal Operator's Manual of instructions will be provided to all terminal users so that operators are fully aware of steps necessary to retrieve the information they are authorized to receive.

b. Software

The Regulations require that "effective and technologically advanced software designs are instituted to prevent unauthorized access" to CHRI.

The following standards have been adopted by the State Central Repository:

- (1.) Establish a terminal identification code number for each remote terminal;
- (2.) The computer should log all inquiries, authorized or unauthorized;
- (3.) Insure that each terminal is defined as to the information it can enter, modify or cancel;
- (4.) Insure that in response to all terminal inquiries, machine-generated reports contain only the information which the seeker is authorized to obtain and only during hours when the terminal is authorized to receive messages;

(5.) Create procedures to allow for suspension of remote terminal access whenever repeated inquiry errors suggest the possibility of tampering.

(6.) Create programs to inform all responsible personnel of unauthorized requests by printing a message on a control terminal.

(7.) Create procedures to deny access to any agency suspended under the user's agreement.

(8.) Create procedures to alert responsible personnel whenever the actual number of inquiries from a remote terminal over a specified time period exceeds the estimated number of inquiries, based on monthly averages from the previous six-month period.

c. Management Control

The management control of the Central Repository is the responsibility of the Department of Public Safety which operates its own computer center. As System Manager of the Arizona Criminal Justice Information System, the Director of DPS will establish the priorities for user access, determine eligibility for direct access, select and dismiss staff and institute the necessary physical security measures which are normally associated with the management of computer operations.

The ACJIS System Manager has the necessary authority and will take the appropriate steps to implement all of the system safeguards required in § 20.21(f)(3)(A)(i) through (vi).

Front end message processors at local or regional levels which have access to CCH at the state level, will be either;

- Owned and operated exclusively by a criminal justice agency;
- Owned and operated by a non-criminal justice government agency on behalf of criminal justice agencies under an agreement which satisfies the requirements of § 20.21(f)(4).

Under ARS 41-2203, the CDS Policy Board has the right to enforce the provisions of § 20.21(f) of the Regulations and to include the provisions thereof in any agreement relating to the processing of or access to criminal history record information.

d. Personnel Clearance System

Under Section IX of the Arizona CDS Master Plan, each criminal justice agency within the state must establish "need-to-know" clearances for terminal operators and agency personnel authorized to access state criminal history information. Agencies directly subject to Subpart B of the Regulations should establish similar clearances for all of their employees

who will be the recipients and/or processors of criminal history information maintained by the agency. These clearances should also be applied to employees of outside entities granted access to criminal information for research, consultation, or the performance of administrative criminal justice services under § 20.21(b)(3) and (4) and § 20.21(d). It will be the responsibility of each criminal justice agency to perform the appropriate clearance procedures, utilizing the services of the local System Security Officer.

Section IX of the Arizona CDS Master Plan requires that a "System Security Officer" be designated in each local terminal agency to assure all necessary physical, personnel, computer and communications safeguards, prescribed by the CDS Policy Board are functioning properly in systems operations.

e. Physical Security Measures

An extensive program to increase the physical security of the DPS compound was undertaken in 1974-75. The program provided:

- An automated security monitoring and access control system based on an IBM System 7. This system provides for the monitoring of fire hazards in the computer center, control of all peripheral access doors and interior doors leading to the computer center, the Central Repository (CIS), the armory, crime laboratory and evidence room.
- An uninterruptible power source was installed which will provide emergency electrical power to support all essential services in the DPS compound including the computer center, and the Central Repository. The DPS also provides essential air conditioning for equipment operations and personnel habitability.

In the other criminal justice agencies throughout the State in which computer terminal hardware is utilized to access state criminal history information, such hardware will be placed within controlled access areas. These areas will be monitored either manually or automatically as the resources of the agency permit. Only authorized terminals may access CCH. All others are denied access via computer hardware and software methods. In 1974-75, a CDS grant provided \$21,000 for the security of those remote terminals. To date twenty-seven (27) small agencies have been assisted by this grant.

All computer facilities housing criminal justice information will employ generally accepted backup procedures and utilize computer tape vaults in separate locations to store file backups.

Regarding manual systems, the following standards apply to the State Central Repository as well as other agencies which are directly subject to the Regulations which maintain manual criminal history information:

(1.) Access Restraints

Record areas should be secured by physical barriers, sign-in procedures, badges, keys, guards, and like controls as necessary.

(2.) Disaster Counter Measures

- Adequate fire detection/suppression devices
- Emergency lighting
- Use of fireproof, lockable filing cabinets
- Other protection as required by the location of the records and environmental hazards

f. Standards for Unauthorized Access

All of the above described approaches, procedures, and techniques, taken together, institute a set of standards for preventing unauthorized access implemented or to be implemented. Arizona is well along in their implementation; these will meet the requirements of § 20.21(f)(2).

g. Training

A program of statewide training will be undertaken under the direction of the ACJIS System Manager. It will include both on-site and centralized training along with appropriate printed material and an Operator's Handbook.

3. Actions Required to Implement this Plan

The CDS Master Plan provides for the security provisions of the Regulations. It will be necessary to continue the implementation of Section III of the CDS Master Plan by carrying out the program outlined in Section VII of that Plan in accordance with the policies and standards contained in Part VIII of that Plan.

When the Security and Privacy Council has compiled all the security standards applicable to criminal history information, it will follow appropriate administrative procedures to establish these standards as "regulations approved or issued by the Governor of the state". § 20.21(f).

4. Accommodation of NLETS Security and Privacy Policies

The National Law Enforcement Telecommunications Systems, Inc., performs a vital function in providing both intrastate and interstate communication facilities for law enforcement. The Board of Directors of NLETS has adopted certain policies regarding the enforcement of the security and privacy

of CHRI carried in the NLETS network and for the implementation and enforcement of the Subpart B and Subpart C of the Regulations.

Inasmuch as the Board of Directors of NLETS is in position to exercise certain sanctions against member agencies and member states — extending to termination of services which have become essential to local law enforcement — it is in the best interests of Arizona to comply with NLETS policy to the maximum extent feasible:

- a. Insure that proper controls are established such that only state authorized criminal justice agencies can access CHRI through NLETS channels. Participation in a Criminal History Record Information User Agreement satisfies this requirement;
- b. Insure that all authorized criminal justice agencies in the state having access to the NLETS network utilize specific message keys and formats for CHRI requests;
- c. Insure that all NLETS users on their intrastate network adhere to the NLETS approved operational procedures required for responding to CHRI requests;
- d. Requests for CHRI, and responses to requests for CHRI, by state-authorized criminal justice agencies are for legitimate purposes;
- e. Agencies requesting CHRI or responding to requests for CHRI must comply with the U.S. Department of Justice Rules and Regulations as they relate to completeness, accuracy, and the dissemination of CHRI;
- f. All NLETS participants must comply with the NLETS policies and procedures for the interstate exchange of CHRI.

E. OBJECTIVE #5 — INDIVIDUAL RIGHTS OF ACCESS AND REVIEW

§ 20.21(g) **Access and Review.** Insure the individual's right to access and review of criminal history information for purposes of accuracy and completeness by instituting procedures so that —

- (1) Any individual shall, upon satisfactory verification of his identity be entitled to review without undue burden to either the criminal justice agency or the individual, any criminal history record information maintained about the individual and obtain a copy thereof when necessary for the purpose of challenge or correction;
- (2) Administrative review and necessary correction of any claim by the individual to whom the information relates that the information is inaccurate or incomplete is provided;

(3) 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;

(4) Upon request, an individual whose record has been corrected shall be given the names of all non-criminal justice agencies to whom the data has been given;

(5) The correcting agency shall notify all criminal justice recipients of corrected information; and

(6) The individual's right to access and review of criminal history record information shall not extend to data contained in intelligence, investigatory, or other related files and shall not be construed to include any other information than that defined by § 20.3(b).

1. Related Federal Law

Section 524(b) of the Crime Control Act of 1973, Public Law 93-83 provides in part:

"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."

2. Arizona Law

ARS 41-1750B-0 The Criminal Identification Section shall:

"Provide information from its records relating to arrests or convictions for public offenses to the subject of such information, or to his attorney at the request of the subject, and when accompanied by proper identification."

3. Scope

The individual's right to access and review of criminal history record information and Subject-in-Process information shall not extend to data contained in intelligence, investigatory, or other related fields and shall not be construed to include any other information than that defined as "criminal history record information" by § 20.3 (b) of the Regulations or Subject-in-Process information as defined in Section II.B.1. of this Plan.

4. Challenge

A "challenge" under this Section is a written contention by an individual that his criminal history record is inaccurate or incomplete; it requires him to give a correct version of his record and explain why he believes his version to be correct.

5. Copy of the Arizona Record

Neither federal law or regulations nor Arizona law or rules prohibit an individual who has properly identified himself from obtaining a copy of a criminal history record of which he is the subject.

Arizona interprets the provisions of 28 CFR 20, § 20.21(g)(1) and § 524(b) of PL 93-83 as assuring the individual that he may obtain a copy at least for the purpose of challenge or correction. There is no way of ascertaining whether or not it is the subject's true intention to challenge the record when he requests a copy. Inasmuch as a person cannot violate his own privacy, there appears to be little cause to restrict a person from obtaining a copy of his own criminal record if he takes the proper steps, including the payment of a reasonable fee, to obtain it, for whatever use he sees fit.

6. Fee

Law Enforcement agencies may charge a fee for providing the individual with a copy of his criminal history record. Such fee should not exceed the reasonable costs involved of making the copies.

7. Procedures

Procedures must be provided to permit a person to:

- a. Obtain, after positive identification, a copy of the Arizona state criminal history record of which he is the subject;
- b. Initiate a challenge to the record;
- c. Provide the administrative machinery for processing the challenges, including provisions for appeal.

8. Obtaining the Arizona Criminal History Record Copy

Any individual after proper identification by fingerprints, or his properly verified attorney, may review his criminal history record at any law enforcement agency in the State which has access to the DPS-CIS Central Repository or the National Crime Information Center CCH File.

- a. The individual must complete a "Review of Criminal Offender Record Information" form (Attachment G). The individual seeking to review his record must have his fingerprints imprinted on this form. The fingerprints must be verified prior to the review of the criminal history record.

b. If the fingerprints of the individual are not on file with the cooperating agency, the fingerprints must be sent to the Criminal Identification Section of the Arizona Department of Public Safety for comparison. To reduce delays, persons residing in the Phoenix area should be encouraged to use the DPS-CIS facility. After verification of the fingerprints the individual or his properly verified attorney will be permitted to review the record, and upon payment of the appropriate fee, obtain a copy thereof.

c. If the cooperating law enforcement agency can make an identification with fingerprints previously taken which are on file locally, and if the FBI identification number of the individual's record is available to that agency, it may make an on-line inquiry of the DPS-CIS Central Repository or NCIC-CCH to obtain the record by computer printout. The subject may then be provided with a copy as in b. above.

It is important to note that these procedures for obtaining a copy of a criminal history record apply only to **an Arizona state criminal record and not federal criminal records**. Procedures for the review and challenge of federal criminal records are governed by PL 93-579, the "Privacy Act of 1974" and federal regulations 28 CFR 16 published August 27, 1975. Federal records are outside the purview of this Plan and of the statutes and regulations on which it is based. Persons seeking records held by other states should be advised to contact the proper authority in that state.

9. Challenge to a Criminal History Record

Challenge to an out-of-state criminal record is the sole responsibility of the subject. The procedures described herein apply only to challenges to Arizona criminal records.

a. To challenge any entry contained in the criminal history record, the "Exception Taken to Criminal Offender Record Information" form (Attachment H) must be properly completed. This form must be signed by the subject of the record to which exceptions were taken.

b. The agency which made the arrest which initiated the challenged portion of the record shall bear the responsibility for investigating the facts of the case. If the subject enters his challenge at a law enforcement agency other than the proper arresting agency, that cooperating agency shall immediately transmit a copy of the challenge, along with a copy of the record and fingerprints to the appropriate arresting agency. In all challenges to in-state records, the original copy of the "Exception Taken to Criminal Record Information" form must be sent to the Arizona Department of Public Safety, Criminal Identification Section.

c. The individual making the challenge bears the responsibility to provide any pertinent information to the arresting agency. Failure to provide sufficient information to verify an alleged discrepancy shall be grounds for dismissal of the challenge.

d. The arresting agency shall, within ninety (90) days, complete its review of the challenge, and shall prepare a "Notice of Results of Audit of Criminal Offender Record Information". The form shall be prepared in triplicate. The original shall be sent to the Arizona Department of Public Safety, Criminal Identification Section. One copy shall be sent to the individual who made the challenge. The remaining copy shall be filed in the arresting agency's file. (Attachment I)

e. When an arresting agency corrects an individual's criminal history record as the result of a challenge, the arresting agency **shall notify the Central Repository**. The arresting agency shall also notify the individual filing the challenge of any non-criminal justice agency that has received incorrect criminal history record information.

10. Administrative Review

If there is factual controversy remaining upon completion of the review of an individual's criminal history record, and it is resolved against the person who made the challenge, the individual is entitled to a review of that decision by someone in the agency of equal or higher rank than the person who made the decision. Each agency shall clearly designate the name or title of the reviewing officer. If the reviewing officer upholds the decision and denies the correction, the individual must be notified in writing.

11. Administrative Appeal

a. Within sixty (60) days after receiving notice of the results of a challenge, an aggrieved party may file a letter of request for review with the Arizona Comprehensive Data System Security and Privacy Council.

b. The request for review shall be mailed to the CDS Security and Privacy Council and the Council shall notify the concerned law enforcement agency of the review by mailing a copy of the request.

c. The CDS Security and Privacy Council shall set a time and date for the hearing and may have the matter heard before the whole Council or may designate one or more of the members as a hearing officer(s) or the Council may engage a hearing officer for purposes of hearing the matter.

d. Notice of the hearing date on the request for review shall be given to the parties by registered or certified mail at least twenty (20) days prior to the date set for the hearing.

e. The hearing shall be conducted in accordance with the Arizona Administrative Procedures Act, ARS 41-1001, et. seq. Parties may be represented by an attorney and shall be afforded an opportunity to respond and present evidence on all issues.

f. The Council may affirm, reverse, modify or supplement the decision of the hearing officer and make such disposition of the case as it determines to be appropriate. The Council shall make its decision within sixty (60) days after the date of the hearing. All parties will be notified of the decision by registered or certified mail.

12. **Implementation**

The procedures for the Individual Rights to Access and Review are effective as of March 15, 1976.

**SECTION V
CERTIFICATION**

Section V CERTIFICATION

A. CERTIFICATION STATEMENT

Attachment J is the certification statement stating the extent to which the Plan procedures have been implemented for agencies covered under Subpart B of the Regulations. Agencies covered under Subpart C of the Regulations will be under contract (Attachment K) with the Central Repository.

B. DISSEMINATION AUTHORIZED TO NON-CRIMINAL JUSTICE AGENCIES

As per the Regulations § 20.22(b)(5) the following is a list of all non-criminal justice agencies within Arizona authorized by statute or executive order to receive criminal history information as of this date.

1. State Agencies Currently Receiving Criminal Records Information for Licensing and/or Employment; all of these state agencies have proper requisite statutory authority for access to criminal records information under 28 CFR 20, § 20.21(b)(2).

- a. Office of Traffic Safety, ARS § 40-60-608C, AARR-R17-4-46
- b. Department of Economic Security, ARS § 46-252
- c. Racing Commission, ARS 5-108, AARR-4-27-03
- d. Corporation Commission, ARS § 44-1941, 1945, 1961, § 4-201
- e. State Department of Insurance, ARS § 20-318
- f. State Department of Health, ARS § 8-506, § 36-428
- g. Department of Public Safety, ARS § 41-1750, AARR-13-5-26
- h. Department of Corrections, ARS § 31-221, § 41-1604

2. State agencies with Current Requisite Statutory Authority to Receive Criminal Records Information; state agencies receiving authorization from Administrative Rules and Regulations qualify under Order 601-75 guidelines because they fulfill the requirements of ARS § 41-1750, and fall under its statutory authorization.

- a. State Bar of Arizona, § 32-272
- b. Board of Barber Examiners, § 32-353
- c. Board of Cosmetology, § 32-552
- d. Board of Podiatry Examiners, § 32-852
- e. Secretary of State — for Collection Agencies, § 32-1023

- f. Registrar of Contractors, § 32-1122
- g. Dental Board, § 32-1232
- h. Board of Medical Examiners, § 32-1423
- i. Naturopathic Board of Examiners, § 32-1556
- j. Board of Nursing, § 32-1664
- k. Board of Dispensing Opticians, § 32-1683
- l. Board of Physical Therapy, § 32-2042
- m. Real Estate Department, § 32-2153
- n. Department of Public Safety for
 - (1) Private Investigators, § 32-2412;
 - (2) Security Guards, § 32-2612
- o. State Banking Department, § 6-817, AARR-4-4-211
- p. Game and Fish Department, § 17-341
- q. State Board of Education, ARS 15-102, R-7-2-401
- r. State Personnel Board, R-2-5-11, § 41-769
- s. Department of Public Welfare, ARS 46-141
- t. Industrial Commission, R-4-13-303
- u. Board of Chiropractic Examiners, § 32-942

C. Attachment L is ARS 41-2201-2206 passed by the Legislature and approved by the Governor on May 31, 1977.

SECTION VI ATTACHMENTS

- A. Federal Register Vol. 40, No. 98 (28 CFR 20) of May 20, 1975, amended as of March 19, 1976**
- B. ARS 41-1750**
- C. ARS 41-1751**
- D. Final Disposition Report Form**
- E. Department of Public Safety — Criminal Identification Section Report of Record Search Form**
- F. Request for Record Information Form**
- G. Review of Criminal Offender Record Information Form**
- H. Exceptions Taken to Criminal Offender Record Information Form**
- I. Notice of Results of Audit of Criminal Offender Record Information Form**
- J. Certification Statements Form**
- K. Criminal History Record Information User Agreement Form**
- L. ARS 41-2201-2206**

RULES AND REGULATIONS

Title 28—Judicial Administration **CHAPTER I—DEPARTMENT OF JUSTICE** **PART 20—CRIMINAL JUSTICE INFORMATION SYSTEMS**

On May 20, 1975, regulations were published in the FEDERAL REGISTER (40 FR 22114) relating to the collection, storage, and dissemination of criminal history record information. Amendments to these regulations were proposed October 24, 1975 (40 FR 49789) based upon a re-evaluation of the dedication requirement contained in § 20.21(f). Hearings on the proposed changes were held November 17, 18, 21 and December 4, 1975. In addition, hearings were held to consider changes to the dissemination provisions of the regulations (40 FR 52846). These hearings were held December 11, 12 and 15, 1975, to consider comments from interested parties on the limitations placed on dissemination of criminal history record information to non-criminal justice agencies. The purpose of the hearings was to determine whether the regulations, as they were drafted, appropriately made the balance between the public's right to know such information with the individual's right of privacy.

As a result of these hearings modifications to the regulations have now been made to better draw this balance. The regulations are based upon section 524(b) of the Crime Control Act of 1973 which provides in relevant part:

"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."

The regulations, as now amended, provide that conviction data may be disseminated without limitation; that criminal history record information relating to the offense for which an individual is currently within the criminal justice system may be disseminated without limitations. Insofar as nonconviction record information is concerned (nonconviction data is defined in § 20.20(k)), the regulations require that after December 31, 1977, most non-criminal justice access would require authorization pursuant to a statute, ordinance, executive order or court rule, decision or order. The regulations no longer require express authority, that is specific language in the authorizing statute or order requiring access to such information, but only that

such dissemination is pursuant to and can be construed from the general requirement in the statute or order. Such statutes include State public record laws which have been interpreted by a State to require that criminal history record information, including nonconviction information, be made available to the public. Determinations as to the purpose for which dissemination of criminal history record information is authorized by State law, executive order, local ordinance, court rule, decision or order will be made by the appropriate State or local officials. The deadline of December 31, 1977, will permit States to obtain the authority, as they believe necessary, to disseminate nonconviction data.

The regulations, as now amended, remove the prohibition that criminal history record information in court records of public judicial proceedings can only be accessed on a chronological basis. § 20.20(b)(3) deletes the words "compiled chronologically". Therefore, court records of public judicial proceedings whether accessed on a chronological basis or on an alphabetical basis are not covered by the regulations.

In addition, the regulations would not prohibit the dissemination of criminal history record information for purposes of international travel (issuance of visas and granting of citizenship). The commentary on selected portions of the regulations have been amended to conform to the changes.

Pursuant to the authority vested in the Law Enforcement Assistance Administration by sections 501 and 524 of the Omnibus Crime Control and Safe Streets Act of 1968, as amended by the Crime Control Act of 1973, Pub. L. 93—83, 87 Stat. 197 (42 U.S.C. 3701 *et seq.*) (Aug. 6, 1973), these amendments to Chapter I of Title 28 of the Code of Federal Regulations are hereby adopted to become final on April 19, 1976. These amendments only amend subparts A and B. Subpart C remains the same.

Subpart A—General Provisions

- Sec.
- 20.1 Purpose.
- 20.2 Authority.
- 20.3 Definitions.

Subpart B—State and Local Criminal History Record Information Systems

- 20.20 Applicability.
- 20.21 Preparation and submission of a Criminal History Record Information Plan.
- 20.22 Certification of Compliance.
- 20.23 Documentation: Approval by LEAA.
- 20.24 State laws on privacy and security.
- 20.25 Penalties.

Subpart C—Federal System and Interstate Exchange of Criminal History Record Information

- 20.30 Applicability.
- 20.31 Responsibilities.
- 20.32 Includable offenses.
- 20.33 Dissemination of criminal history record information.
- 20.34 Individual's right to access criminal history record information.
- 20.35 National Crime Information Center Advisory Policy Board.
- 20.36 Participation in the Computerized Criminal History Program.
- 20.37 Responsibility for accuracy, completeness, currency.
- 20.38 Sanction for noncompliance.

AUTHORITY: Pub. L. 93-83, 87 Stat. 197 (42 USC 3701, *et seq.*; 28 USC 534), Pub. L. 92-544, 86 Stat. 1115.

Subpart A—General Provisions

§ 20.1 Purpose.

It is the purpose of these regulations to assure that criminal history record information wherever it appears is collected, stored, and disseminated in a manner to insure the completeness, integrity, accuracy and security of such information and to protect individual privacy.

§ 20.2 Authority.

These regulations are issued pursuant to sections 501 and 524(b) of the Omnibus Crime Control and Safe Streets Act of 1968, as amended by the Crime Control Act of 1973, Pub. L. 93-83, 87 Stat. 197, 42 USC 3701, *et seq.* (Act), 28 USC 534, and Pub. L. 92-544, 86 Stat. 1115.

§ 20.3 Definitions.

As used in these regulations:

(a) "Criminal history record information system" means a system including the equipment, facilities, procedures, agreements, and organizations thereof, for the collection, processing, preservation or dissemination of criminal history record information.

(b) "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 to the extent that such information does not indicate involvement of the individual in the criminal justice system.

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

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

(e) "Disposition" means information disclosing that criminal proceedings have been concluded, including information disclosing that the police have elected not to refer a matter to a prosecutor or that a prosecutor has elected not to commence criminal proceedings and also disclosing the nature of the termination in the proceedings; or information disclosing that proceedings have been indefinitely postponed and also disclosing the reason for such postponement. Dispositions shall include, but not be limited to, acquittal, acquittal by reason of insanity, acquittal by reason of mental incompetence, case continued without finding, charge dismissed, charge dismissed due to insanity, charge dismissed due to mental incompetency, charge still pending due to insanity, charge still pending due to mental incompetence, guilty plea, nolle prosequi, no paper, nolo contendere plea, convicted, youthful offender determination, deceased, deferred disposition, dismissed—civil action, found insane, found mentally incompetent, pardoned, probation before conviction, sentence commuted, adjudication withheld, mistrial—defendant discharged, executive clemency, placed on probation, paroled, or released from correctional supervision.

(f) "Statute" means an Act of Congress or State legislature or a provision of the Constitution of the United States or of a State.

(g) "State" means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, and any territory or possession of the United States.

(h) An "executive order" means an order of the President of the United States or the Chief Executive of a State which has the force of law and which is published in a manner permitting regular public access thereto.

(i) "Act" means the Omnibus Crime Control and Safe Streets Act, 42 USC 3701, *et seq.*, as amended.

(j) "Department of Justice criminal history record information system" means the Identification Division and the Computerized Criminal History File systems operated by the Federal Bureau of Investigation.

(k) "Nonconviction data" means arrest information without disposition if an interval of one year has elapsed from the date of arrest and no active prosecution of the charge is pending; or information disclosing that the police have elected not to refer a

matter to a prosecutor, or that a prosecutor has elected not to commence criminal proceedings, or that proceedings have been indefinitely postponed, as well as all acquittals and all dismissals.

(l) "Direct access" means having the authority to access the criminal history record data base, whether by manual or automated methods.

Subpart B—State and Local Criminal History Record Information Systems

§ 20.20 Applicability.

(a) The regulations in this subpart apply to all State and local agencies and individuals collecting, storing, or disseminating criminal history record information processed by manual or automated operations where such collection, storage, or dissemination has been funded in whole or in part with funds made available by the Law Enforcement Assistance Administration subsequent to July 1, 1973, pursuant to Title I of the Act. Use of information obtained from the FBI Identification Division or the FBI/NCIC system shall also be subject to limitations contained in Subpart C.

(b) The regulations in this subpart shall not apply to criminal history record information contained in: (1) posters, announcements, or lists for identifying or apprehending fugitives or wanted persons; (2) original records of entry such as police blotters maintained by criminal justice agencies, compiled chronologically and required by law or long standing custom to be made public, if such records are organized on a chronological basis; (3) court records of public judicial proceedings; (4) published court or administrative opinions or public judicial, administrative or legislative proceedings; (5) records of traffic offenses maintained by State departments of transportation, motor vehicles or the equivalent thereof for the purpose of regulating the issuance, suspension, revocation, or renewal of driver's, pilot's or other operators' licenses; (6) announcements of executive clemency.

(c) Nothing in these regulations prevents a criminal justice agency from disclosing to the public criminal history record information related to the offense for which an individual is currently within the criminal justice system. Nor is a criminal justice agency prohibited from confirming prior criminal history record information to members of the news media or any other person, upon specific inquiry as to whether a named individual was arrested, detained, indicted, or whether an information or other formal charge was filed, on a specified date, if the arrest record information or criminal record information disclosed is based on data excluded by paragraph (b) of this section. The regulations do not prohibit the dissemination of criminal history record information for purposes of international travel, such as issuing visas and granting of citizenship.

§ 20.21 Preparation and submission of a Criminal History Record Information Plan.

A plan shall be submitted to LEAA by each State on March 16, 1976, to set forth all operational procedures, except those portions relating to dissemination and security.

A supplemental plan covering these portions shall be submitted no later than 90 days after promulgation of these amended regulations. The plan shall set forth operational procedures to—

(a) *Completeness and accuracy.* Insure that criminal history record information is complete and accurate.

(1) Complete records should be maintained at a central State repository. To be complete, a record maintained at a central State repository which contains information that an individual has been arrested, and which is available for dissemination, must contain information of any dispositions occurring within the State within 90 days after the disposition has occurred. The above shall apply to all arrests occurring subsequent to the effective date of these regulations. 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. 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.

(2) To be accurate means that no record containing criminal history record information shall contain erroneous information. To accomplish this end, criminal justice agencies shall institute a process of data collection, entry, storage, and systematic audit that will minimize the possibility of recording and storing inaccurate information and upon finding inaccurate information of a material nature, shall notify all criminal justice agencies known to have received such information.

(b) *Limitations on dissemination.* By December 31, 1977, insure that dissemination of nonconviction data has been limited, whether directly or through any intermediary only to:

(1) Criminal justice agencies, for purposes of the administration of criminal justice and criminal justice agency employment;

(2) 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;

(3) 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 that security and confidentiality of the data consistent with these regulations, and provide sanctions for violation thereof;

(4) 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.

These dissemination limitations do not apply to conviction data.

(c) *General policies on use and dissemination.* (1) Use of criminal history record information disseminated to noncriminal justice agencies shall be limited to the purpose for which it was given.

(2) No agency or individual shall confirm the existence or nonexistence of criminal history record information to any person or agency that would not be eligible to receive the information itself.

(3) Subsection (b) does not mandate dissemination of criminal history record information to any agency or individual. States and local governments will determine the purposes for which dissemination of criminal history record information is authorized by State law, executive order, local ordinance, court rule, decision or order.

(d) *Juvenile records.* Insure that dissemination of records concerning proceedings relating to the adjudication of a juvenile as delinquent or in need of supervision (or the equivalent) to noncriminal justice agencies is prohibited, unless a statute, court order, rule or court decision specifically authorizes dissemination of juvenile records, except to the same extent as criminal history records may be disseminated as provided in § 20.21(b)(3) and (4).

(e) *Audit.* 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. Such records shall include, but are not limited to, the names of all persons or agencies to whom information is disseminated and the date upon which such information is disseminated. The reporting of a criminal justice transaction to a State, local or Federal repository is not a dissemination of information.

(f) *Security.* Wherever criminal history record information is collected, stored, or disseminated, each State shall insure that the following requirements are satisfied by security standards established by State legislation, or in the absence of such legislation, by regulations approved or issued by the Governor of the State.

(1) Where computerized data processing is employed, effective and technologically advanced software and hardware designs are instituted to prevent unauthorized access to such information.

(2) Access to criminal history record information system facilities, systems operating environments, data file contents whether while in use or when stored in a media library, and system documentation is restricted to authorized organizations and personnel.

(3)(A) Computer operations, whether dedicated or shared, which support criminal justice information systems, operate in accordance with procedures developed or approved by the participating criminal justice agencies that assure that:

(i) Criminal history record information is stored by the computer in such manner that it cannot be modified, destroyed, accessed, changed, purged, or overlaid in any fashion by non-criminal justice terminals.

(ii) Operation programs are used that will prohibit inquiry, record updates, or destruction of records, from any terminal other than criminal justice system terminals which are so designated.

(iii) The destruction of records is limited to designated terminals under the direct control of the criminal justice agency responsible for creating or storing the criminal history record information.

(iv) Operational programs are used to detect and store for the output of designated criminal justice agency employees all unauthorized attempts to penetrate any criminal history record information system, program or file.

(v) The programs specified in (ii) and (iv) of this subsection are known only to criminal justice agency employees responsible for criminal history record information system control or individuals and agencies pursuant to a specific agreement with the criminal justice agency to provide such programs and the program(s) are kept continuously under maximum security conditions.

(vi) Procedures are instituted to assure that an individual or agency authorized direct access is responsible for *A* the physical security of criminal history record information under its control or in its custody and *B* the protection of such information from unauthorized access, disclosure or dissemination.

(vii) Procedures are instituted to protect any central repository of criminal history record information from unauthorized access, theft, sabotage, fire, flood, wind, or other natural or manmade disasters.

(B) A criminal justice agency shall have the right to audit, monitor and inspect procedures established above.

(4) The criminal justice agency will:

(A) Screen and have the right to reject for employment, based on good cause, all personnel to be authorized to have direct access to criminal history record information.

(B) Have the right to initiate or cause to be initiated administrative action leading to the transfer or removal of personnel authorized to have direct access to such information where such personnel violate the provisions of these regulations or other security requirements established for the collection, storage, or dissemination of criminal history record information.

(C) Institute procedures, where computer processing is not utilized, to assure that an individual or agency authorized direct access is responsible for (i) the physical

security of criminal history record information under its control or in its custody and (ii) the protection of such information from unauthorized access, disclosure, or dissemination.

(D) Institute procedures, where computer processing is not utilized, to protect any central repository of criminal history record information from unauthorized access, theft, sabotage, fire, flood, wind, or other natural or man-made disasters.

(E) Provide that direct access to criminal history record information shall be available only to authorized officers or employees of a criminal justice agency and, as necessary, other authorized personnel essential to the proper operation of the criminal history record information system.

(5) Each employee working with or having access to criminal history record information shall be made familiar with the substance and intent of these regulations.

(g) *Access and review.* Insure the individual's right to access and review of criminal history information for purposes of accuracy and completeness by instituting procedures so that—

(1) Any individual shall, upon satisfactory verification of his identity, be entitled to review without undue burden to either the criminal justice agency or the individual, any criminal history record information maintained about the individual and obtain a copy thereof when necessary for the purpose of challenge or correction;

(2) Administrative review and necessary correction of any claim by the individual to whom the information relates that the information is inaccurate or incomplete is provided;

(3) 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;

(4) Upon request, an individual whose record has been corrected shall be given the names of all non-criminal justice agencies to whom the data has been given;

(5) The correcting agency shall notify all criminal justice recipients of corrected information; and

(6) The individual's right to access and review of criminal history record information shall not extend to data contained in intelligence, investigatory, or other related files and shall not be construed to include any other information than that defined by § 20.3(b).

§ 20.22 Certification of Compliance.

(a) Each State to which these regulations are applicable shall with the submission of its plan provide a certification that to the maximum extent feasible action has been taken to comply with the procedures set forth in the plan. Maximum extent feasible, in

this subsection, means actions which can be taken to comply with the procedures set forth in the plan that do not require additional legislative authority or involve unreasonable cost or do not exceed existing technical ability.

(b) The certification shall include—

(1) An outline of the action which has been instituted. At a minimum, the requirements of access and review under § 20.21(g) must be completely operational;

(2) A description of any legislation or executive order, or attempts to obtain such authority that has been instituted to comply with these regulations;

(3) A description of the steps taken to overcome any fiscal, technical, and administrative barriers to the development of complete and accurate criminal history record information;

(4) A description of existing system capability and steps being taken to upgrade such capabilities to meet the requirements of these regulations; and

(5) A listing setting forth categories of non-criminal justice dissemination. See § 20.21(b).

§ 20.23 Documentation: Approval by LEAA.

Within 90 days of the receipt of the plan, LEAA shall approve or disapprove the adequacy of the provisions of the plan and certification. Evaluation of the plan by LEAA will be based upon whether the procedures set forth will accomplish the required objectives. The evaluation of the certification(s) will be based upon whether a good faith effort has been shown to initiate and/or further compliance with the plan and regulations. All procedures in the approved plan must be fully operational and implemented by December 31, 1977. A final certification shall be submitted in December 1977.

§ 20.24 State laws on privacy and security.

Where a State originating criminal history record information provides for sealing or purging thereof, nothing in these regulations shall be construed to prevent any other State receiving such information, upon notification, from complying with the originating State's sealing or purging requirements.

§ 20.25 Penalties.

Any agency or individual violating subpart B of these regulations shall be subject to a fine not to exceed \$10,000. In addition, LEAA may initiate fund cut-off procedures against recipients of LEAA assistance.

RICHARD W. VELDE,
Administrator

Subpart C—Federal System and Interstate Exchange of Criminal History Record Information

§ 20.30 Applicability.

The provisions of this subpart of the regulations apply to any Department of Justice criminal history record information system that serves criminal justice agencies in two or more states and to Federal, state and local criminal justice agencies to the extent that they utilize the services of Department of Justice criminal history record information systems. These regulations are applicable to both manual and automated systems.

§ 20.31 Responsibilities

(a) The Federal Bureau of Investigation (FBI) shall operate the National Crime Information Center (NCIC), the computerized information system which includes telecommunications lines and any message switching facilities which are authorized by law or regulation to link local, state and Federal criminal justice agencies for the purpose of exchanging NCIC-related information. Such information includes information in the Computerized Criminal History (CCH) File, a cooperative Federal-State program for the interstate exchange of criminal history record information. CCH shall provide a central repository and index of criminal history record information for the purpose of facilitating the interstate exchange of such information among criminal justice agencies.

(b) The FBI shall operate the Identification Division to perform identification and criminal history record information functions for Federal, state and local criminal justice agencies, and for noncriminal justice agencies and other entities where authorized by Federal statute, state statute pursuant to Public Law 92-544 (86 Stat. 1115), Presidential executive order, or regulation of the Attorney General of the United States.

(c) The FBI Identification Division shall maintain the master fingerprint files on all offenders included in the NCIC/CCH File for the purposes of determining first offender status and to identify those offenders who are unknown in states where they become criminally active but known in other states through prior criminal history records.

§ 20.32 Includable offenses.

(a) Criminal history record information maintained in any Department of Justice criminal history record information system shall include serious and/or significant offenses.

(b) Excluded from such a system are arrests and court actions limited only to nonserious charges, e.g., drunkenness, vagrancy, disturbing the peace, curfew violation, loitering, false fire alarm, nonspecific charges of suspicion or investigation, traffic violations (except data will be included on arrests for manslaughter, driving under the influence of drugs or liquor, and hit and run).

(b) Excluded from such a system are arrests and court actions limited only to nonserious charges, e.g., drunkenness, vagrancy, disturbing the peace, curfew violation, loitering, false fire alarm, nonspecific charges of suspicion or investigation, traffic violations (except data will be included on arrests for manslaughter, driving under the influence of drugs or liquor, and hit and run). Offenses committed by juvenile offenders shall also be excluded unless a juvenile offender is tried in court as an adult.

(c) The exclusions enumerated above shall not apply to Federal manual criminal history record information collected, maintained and compiled by the FBI prior to the effective date of these Regulations.

§ 20.33 Dissemination of criminal history record information.

(a) Criminal history record information contained in any Department of Justice criminal history record information system will be made available:

(1) To criminal justice agencies for criminal justice purposes; and

(2) To Federal agencies authorized to receive it pursuant to Federal statute or Executive order.

(3) Pursuant to Public Law 92-544 (86 Stat. 115) for use in connection with licensing or local/state employment or for other uses only if such dissemination is authorized by Federal or state statutes and approved by the Attorney General of the United States. When no active prosecution of the charge is known to be pending arrest data more than one year old will not be disseminated pursuant to this subsection unless accompanied by information relating to the disposition of that arrest.

(4) For issuance of press releases and publicity designed to effect the apprehension of wanted persons in connection with serious or significant offenses.

(b) The exchange of criminal history record information authorized by paragraph (a) of this section is subject to cancellation if dissemination is made outside the receiving departments or related agencies.

(c) Nothing in these regulations prevents a criminal justice agency from disclosing to the public factual information concerning the status of an investigation, the apprehension, arrest, release, or prosecution of an individual, the adjudication of charges, or the correctional status of an individual, which is reasonably contemporaneous with the event to which the information relates.

§ 20.34 Individual's right to access criminal history record information.

(a) Any individual, upon request, upon satisfactory verification of his identity by fingerprint comparison and upon payment of any required processing fee, may review criminal history record information maintained about him in a Department of Justice criminal history record information system.

(b) If, after reviewing his identification record, the subject thereof believes that it is

incorrect or incomplete in any respect and wishes changes, corrections or updating of the alleged deficiency, he must make application directly to the contributor of the questioned information. If the contributor corrects the record, it shall promptly notify the FBI and, upon receipt of such a notification, the FBI will make any changes necessary in accordance with the correction supplied by the contributor of the original information.

§ 20.35 National Crime Information Center Advisory Policy Board.

There is established an NCIC Advisory Policy Board whose purpose is to recommend to the Director, FBI, general policies with respect to the philosophy, concept and operational principles of NCIC, particularly its relationships with local and state systems relating to the collection, processing, storage, dissemination and use of criminal history record information contained in the CCH File.

(a)(1) The Board shall be composed of twenty-six members, twenty of whom are elected by the NCIC users from across the entire United States and six who are appointed by the Director of the FBI. The six appointed members, two each from the judicial, the corrections and the prosecutive sectors of the criminal justice community, shall serve for an indeterminate period of time. The twenty elected members shall serve for a term of two years commencing on January 5th of each odd numbered year.

(2) The Board shall be representative of the entire criminal justice community at the state and local levels and shall include representation from law enforcement, the courts and corrections segments of this community.

(b) The Board shall review and consider rules, regulations and procedures for the operation of the NCIC.

(c) The Board shall consider operational needs of criminal justice agencies in light of public policies, and local, state and Federal statutes and these Regulations.

(d) The Board shall review and consider security and privacy aspects of the NCIC system and shall have a standing Security and Confidentiality Committee to provide input and recommendations to the Board concerning security and privacy of the NCIC system on a continuing basis.

(e) The Board shall recommend standards for participation by criminal justice agencies in the NCIC system.

(f) The Board shall report directly to the Director of the FBI or his designated appointee.

(g) The Board shall operate within the purview of the Federal Advisory Committee Act, Public Law 92-463 86 Stat. 770.

(h) The Director, FBI, shall not adopt recommendations of the Board which would be in violation of these Regulations.

§ 20.36 Participation in the Computerized Criminal History Program.

(a) For the purpose of acquiring and retaining direct access to CCH File each criminal justice agency shall execute a signed agreement with the Director, FBI, to abide by all present rules, policies and procedures of the NCIC, as well as any rules, policies and procedures hereinafter approved by the NCIC Advisory Policy Board and adopted by the NCIC.

(b) Entry of criminal history record information into the CCH File will be accepted only from an authorized state or Federal criminal justice control terminal. Terminal devices in other authorized criminal justice agencies will be limited to inquiries.

§ 20.37 Responsibility for accuracy, completeness, currency.

It shall be the responsibility of each criminal justice agency contributing data to any Department of Justice criminal history record information system to assure that information on individuals is kept complete, accurate and current so that all such records shall contain to the maximum extent feasible dispositions for all arrest data included therein. Dispositions should be submitted by criminal justice agencies within 120 days after the disposition has occurred.

§ 20.38 Sanction for noncompliance.

The services of Department of Justice criminal history record information systems are subject to cancellation in regard to any agency or entity which fails to comply with the provisions of Subpart C.

EDWARD H. LEVI
Attorney General

MAY 15, 1975.

RICHARD W. VELDE
*Administrator, Law Enforcement
Assistance Administration*

MAY 15, 1975.

ARIZONA REVISED STATUTES**§ 41-1750. Criminal identification section; duties**

A. There shall be a criminal identification section within the department of public safety.

B. The criminal identification section shall:

1. Procure and maintain records of photographs, descriptions, fingerprints, dispositions and such other information as may be pertinent to all persons who have been arrested for or convicted of a public offense within the state.

2. Collect information concerning the number and nature of offenses known to have been committed in this state, of the legal steps taken in connection therewith, and such other information as shall be useful in the study of crime in the administration of justice.

3. Cooperate with the criminal identification bureaus in other states and with the appropriate agency of the federal government in the exchange of information pertinent to violators of the law. In addition, the criminal identification section shall provide for the rapid exchange of information concerning the commission of crime and the detection of violators of the law, between the law enforcement agencies of this state and its political subdivisions and the law enforcement agencies of other states and of the federal government.

4. Furnish assistance to peace officers throughout the state in crime scene investigation for the detection of latent fingerprints, and in the comparison thereof.

5. Provide information from its records to law enforcement agencies of the state or its political subdivisions upon request by the chief officer of such agency or his authorized representative. Such information shall be used only for purposes of law enforcement.

6. Provide information from its records to courts, prosecutors or correctional agencies of the state or its political subdivisions upon request by the chief officer of such agency or his authorized representative. Such information shall be used only for purposes of the criminal justice system.

7. Provide information from its records relating to convictions for public offenses to nonlaw enforcement agencies of the state or its political subdivisions upon request by the chief officer of such agency or his authorized representative, for the purpose of evaluating the fitness of prospective employees of such agency. Such information shall be used only for the purpose of such evaluation.

8. Provide information from its records relating to convictions for public offenses to licensing and regulatory agencies of the state or its political subdivisions upon request by the chief officer of such agency or his authorized representative, for the purpose of evaluating the fitness of prospective licensees. Such information shall be used only for the purpose of such evaluation.

9. Provide information from its records relating to arrests or convictions for public offenses to the subject of such information, or to his attorney at the request of the subject, and when accompanied by proper identification.

C. The chief officers of law enforcement agencies of the state or its political subdivisions shall provide to the criminal identification section such information concerning crimes and persons arrested for or convicted of public offenses within the state as the chief of the criminal identification section, with the approval of the director, shall deem useful for the study or prevention of crime and for the administration of justice.

D. Any person who releases or procures the release of information held by the criminal identification section other than as provided by this section, or who uses such information for a purpose other than is provided by this section, is guilty of a misdemeanor.

E. The chief of the criminal identification section may, with the written approval of the director and in the manner prescribed by law, remove and destroy such records as he determines are no longer of value in the detection or prevention of crime.

F. The chief of the criminal identification section, subject to the approval of the director, shall make and issue rules and regulations relating to the procurement and dissemination of information, in the manner prescribed by law.

G. All nonlaw enforcement agencies of the state or its political subdivisions may establish by rule, regulation or ordinance the need for fingerprint or background investigations for purposes of employment or licensing and may, thereafter, utilize the criminal identification section of the department of public safety in accordance with subsection F.

ARIZONA REVISED STATUTES**§ 41-1751. Reporting court dispositions to department of public safety**

Every magistrate, or judge of a court, or clerk of a court of record who is responsible for court records in this state shall furnish to the criminal identification section of the department of public safety information pertaining to all court dispositions of criminal matters, where incarceration or fingerprinting of the person occurred, including guilty pleas, convictions, acquittals, probations granted and pleas of guilty to reduced charges within ten days of the final disposition. Such information shall be submitted on a form and in accordance with rules approved by the supreme court of the state.

INSTRUCTIONS

1. The purpose of this report is to record the initial data of an individual's arrest and thereafter secure the FINAL DISPOSITION of the arrest at the earliest possible time from either the arresting agency, the prosecutor, or the court having jurisdiction. (INTERIM DISPOSITION INFORMATION, for example, RELEASED ON BOND, SHOULD NOT BE SUBMITTED.) THE SUBJECT'S NAME, CONTRIBUTOR, AND ARREST NUMBER should be exactly the same as they appear on the fingerprint card IN THE FILES OF THE CIS. The FBI number should be indicated, if known. The agency ultimately making final disposition will complete and mail the form to: THE DEPARTMENT OF PUBLIC SAFETY, CRIMINAL IDENTIFICATION SECTION, 2010 W. ENCANTO BLVD., PHOENIX, ARIZONA 85005. CIS will forward a copy to the FBI for their files.
2. THE ARRESTING AGENCY should fill in all of the arrest data on the left side of this form and obtain the finger impressions of the right four fingers simultaneously. This should be done at the same time as the full set of fingerprints are taken on the arrest fingerprint card. If the arrest is disposed of by the arresting agency, as where the arrestee is released without charge, then the arresting agency should fill in this final disposition and mail this form to the CIS. Of course, if the final disposition is known when the arrest fingerprint card is submitted, it should be noted thereon and this form is then unnecessary. In the event the case goes to the prosecutor, this form should be forwarded to the prosecutor with the arrestee's file.
3. THE PROSECUTOR should complete the form to show final disposition at the prosecution level if the matter is not being referred for court action and thereafter submit the form directly to the Criminal Identification Section. If court action is required, the prosecutor should forward this form with the case file to the court having jurisdiction.
4. THE COURT should complete this form as to final court disposition such as when the arrested person is acquitted, the case is dismissed, on conviction, and when sentence is imposed or sentence is suspended and the person is placed on probation. Each court should place their case number in the appropriate box in the upper right-hand corner.
5. MODIFIED CHARGES: When the arrested person is convicted or enters a guilty plea to a lesser or different offense than that charged when originally arrested, this information should be clearly indicated on this form.
6. EXPUNGEMENT: If subsequent action is taken to seal or expunge a record, attach a certified or authenticated copy of the court order to this form so that CIS can return the arrestee's fingerprints to the original contributor.
7. It is VITALLY IMPORTANT for the completion of the subject's record in the Criminal Identification Section files that the FINAL DISPOSITION REPORT be submitted in every instance where fingerprints are previously forwarded without final disposition noted thereon.

ARIZONA DEPARTMENT OF PUBLIC SAFETY
CRIMINAL IDENTIFICATION SECTION

REPORT OF RECORD SEARCH

Date

Subject of Search: _____

Date of Birth: _____

A search of the Department of Public Safety's Arizona Criminal History files reveals that there is no record of any misdemeanor or felony convictions on the above-named person.

Chief

Criminal Identification Section
Arizona Department of Public Safety

SAMPLE

REQUEST FOR RECORD INFORMATION

PART I.

NAME/ _____

DOB/ _____ SOC/ _____

AKA/ _____ SEX/RAC _____

SID _____ FBI _____

REQUESTED BY _____

PURPOSE _____

PART II.

REQUESTOR IS: CRIMINAL JUSTICE AGENCY

 NON-CRIMINAL JUSTICE AGENCY

 PRIVATE CITIZEN

INFORMATION INDEXED AS

LAW ENFORCEMENT RECORDS	<input type="checkbox"/>	ORIGINAL RECORDS OF ENTRY	<input type="checkbox"/>
CONVICTION DATA	<input type="checkbox"/>	CHRONOLOGICAL ACCESS	<input type="checkbox"/>
NONCONVICTION DATA	<input type="checkbox"/>	ALPHABETICAL ACCESS	<input type="checkbox"/>
SUBJECT-IN-PROCESS INFORMATION	<input type="checkbox"/>	JUVENILE RECORDS	<input type="checkbox"/>
PUBLIC RECORDS	<input type="checkbox"/>		

SOURCE ACCESSED:

NCIC	<input type="checkbox"/>	CCH	<input type="checkbox"/>	LOCAL RECORDS	<input type="checkbox"/>
ACIC	<input type="checkbox"/>	STATE RECORDS	<input type="checkbox"/>		

INFORMATION PROVIDED? YES _____ NO _____

CHECKED BY _____ DATE _____

REVIEW OF CRIMINAL OFFENDER RECORD INFORMATION

CIS NUMBER

name of reviewing individual

name of individual to whom record relates

copy of record desired: Yes No

signature of individual to whom copy released

date copy obtained

name and ID No. of employee releasing information

NOTICE TO REVIEWING INDIVIDUAL

The record to be reviewed consists only of arrests and dispositions occurring in the State of Arizona. You have the right to challenge any entry on the record which you believe to be incorrect. To do so, you must complete DPS Form 30.60.07. An audit of this record will then be conducted.

THIS FORM WILL BECOME A PERMANENT PART OF THE ABOVE MENTIONED RECORD.

prints taken by

date

SAMPLE

right four fingers taken simultaneously

EXCEPTIONS TAKEN TO CRIMINAL OFFENDER RECORD INFORMATION

Name of Individual Submitting Exceptions

Originator's Case Number

Name of Subject of Record

Date of Birth

CIS Number

Date Exceptions Submitted

ID No. of Employee
Accepting this Form

SUMMARY OF EXCEPTIONS AND REASONS THEREFORE _____

SAMPLE

VERIFICATION:

I affirm that I have taken the above-described exceptions, that those exceptions are taken in good faith, and that they are to the best of my knowledge and belief true.

Signature of Subject of Record

Date

NAME AND COMPLETE MAILING ADDRESS OF PERSON SUBMITTING THIS FORM SHALL BE RECORDED ON THE OTHER SIDE OF THIS FORM.

NOTICE OF RESULTS OF AUDIT
OF CRIMINAL OFFENDER RECORD INFORMATION

TO: _____

Pursuant to exceptions taken on _____ 19_____, by _____
_____ to criminal offender record information contained in CIS jacket
No. _____, originator's case number _____, an audit of the information has
been conducted and, in accordance with the results of that audit, the exceptions have been _____
_____. The following actions have been
taken, or now are in progress, to implement the audit's findings: _____

SAMPLE

Signature of Records' Custodian

Date

U. S. DEPARTMENT OF JUSTICE LAW ENFORCEMENT ASSISTANCE ADMINISTRATION NATIONAL CRIMINAL JUSTICE INFORMATION AND STATISTICS SERVICE WASHINGTON, D. C. 20531		INFORMATION STATEMENT (28 CFR 20.1 - 20.38)	INSTRUCTIONS Please provide the following information, complete the attached certification form and return all parts to the address at the left.
NAME/ADDRESS OF SUBMITTING AGENCY		APPLICABLE STATE	DATE PREPARED
		CONTACT NAME	TEL. NO. (Give Area Code)
1. Does your agency "collect, store, or disseminate criminal history record information processed by either manual or automated operations?" "Criminal history record information" means information collected by criminal justice agencies on individuals which consist 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 to the extent that such information does not indicate involvement of the individual in the criminal justice system.			
YES <input type="checkbox"/> NO <input type="checkbox"/>			
2. If the answer above was "Yes," have LEAA funds been made available to the agency subsequent to July 1, 1973 for the collection, storage or dissemination of information?			
YES <input type="checkbox"/> NO <input type="checkbox"/>			
3. Indicate the type of agency:			
<input type="checkbox"/> PROSECUTION <input type="checkbox"/> PUBLIC DEFENDER <input type="checkbox"/> POLICE <input type="checkbox"/> COURTS <input type="checkbox"/> CORRECTIONS			
4. Indicate the type of system:		5. Is the system automated?	
<input type="checkbox"/> SUBJECT IN PROCESS <input type="checkbox"/> CRIMINAL HISTORY		<input type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> PARTIAL	
6. Does the system(s) exchange information with other systems? If "Yes," specify which other systems:			
<input type="checkbox"/> YES <input type="checkbox"/> NO <input type="checkbox"/> REGIONAL <input type="checkbox"/> CENTRAL STATE REPOSITORY <input type="checkbox"/> NCIC <input type="checkbox"/> OTHER (specify) _____			
7. Indicate population of primary geographic jurisdiction being served:		8. Indicate approximate number of subjects included in system:	
_____		<input type="checkbox"/> 0-5,000 <input type="checkbox"/> 5,000-25,000 <input type="checkbox"/> 25,000-100,000 <input type="checkbox"/> 100,000-500,000 <input type="checkbox"/> MORE THAN 500,000	
9. Name of authorized agency official		10. Title	
11. Agency name and address		12. Tel. No. (give Area Code)	
		13. Signature of authorized official	

OPERATIONAL PROCEDURES	CHECK MARKS			DATES
	REASONS FOR NON-IMPLEMENTATION			ESTIMATED IMPLEMENTATION DATE
	COST	TECHNICAL	LACK OF AUTHORITY	
*Security				
Executive/Statutory Designation of Responsible Criminal Justice Agency				
Prevention of Unauthorized Access:				
Hardware Design				
Software Design				
Dedicated Hardware:				
Terminals				
Communications Control				
Processor				
Storage Devices				
Criminal Justice Agency Authority:				
Computer Operations Policy				
Access to Work Areas				
Selection and Supervision of Personnel				
Assignment of Administrative Responsibility:				
Physical Security				
Unauthorized Access				
Physical Protection Against:				
Access to Equipment				
Theft, Sabotage				
Fire, Flood, Other Natural Disasters				
Employee Training Program				
Individual Right of Access				
Rules for Access				
Point of Review and Mechanism				
Challenge by Individual				
Administrative Review				
Administrative Appeal				
Correction/Notification of Error				
CERTIFICATION	SIGNATURE <i>(Head of State Agency designated to be responsible for these regulations)</i>			
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 for the State.				
REMARKS				

CRIMINAL HISTORY RECORD INFORMATION USER AGREEMENT

THIS AGREEMENT is made and entered into by the ARIZONA DEPARTMENT OF PUBLIC SAFETY, hereinafter referred to as "DPS", and _____, hereinafter referred to as "USER". DPS is the State Terminal Control Agency for the Arizona Crime Information Center and State Central Repository under the authority of the Comprehensive Data Systems Policy Board and A.R.S. § 41-2201 et seq.

User is:

A criminal justice agency as defined in 28 CFR, Part 20;

OR

A non-criminal justice agency authorized to receive criminal history record information pursuant to 28 CFR, Part 20.

DPS and User hereby agree to exchange such criminal history record information, wanted persons information, and missing persons information as is available in the State of Arizona Central Repository, The Arizona Crime Information Center, in the files of User, or the National Crime Information Center of the Federal Bureau of Investigation, including Computerized Criminal Histories, subject to the terms and conditions listed below.

TERMS AND CONDITIONS

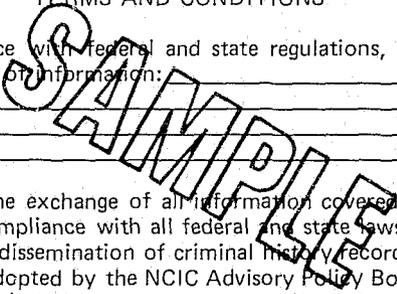
1. Information. In accordance with federal and state regulations, DPS agrees to furnish User with the following type(s) of information: _____

2. Rules and Regulations. The exchange of all information covered by the terms of this agreement shall be in strict compliance with all federal and state laws and regulations relating to the collection, storage, or dissemination of criminal history record information; with all rules, procedures, and policies adopted by the NCIC Advisory Policy Board in regard to information furnished through the FBI/NCIC CCH program; and with all rules and regulations adopted by the Comprehensive Data Systems Policy Board for the Arizona Criminal Justice Information System. User has the burden of giving notice of the requirements of all the above-named rules and regulations to its employees and to other agencies or individuals to whom User might disseminate information derived pursuant to this agreement.

3. Security and Privacy.

A. Purpose. User agrees that the use of information received under the terms of this agreement shall be limited to the following specific purpose(s): _____

B. System Security Officer. User shall designate an official System Security Officer who shall be responsible for ensuring compliance with Section 2 above, and who shall grant authorization to those employees who will have access to criminal history record information.



4. **Audits.** User hereby agrees to make its records available to DPS for the purpose of conducting periodic audits of User's compliance with all laws and regulations regarding the processing of information furnished to User under the terms of this agreement. User agrees to keep such records as DPS may from time to time direct in order to facilitate such audits. In addition, User will cooperate with directives issued by the State Terminal Control Officer to assure reliability of data.
5. **Sanctions.**
 - A. **Cancellation.** Either DPS or User may cancel this agreement upon thirty days notice to the other party in writing.
 - B. **Suspension of Service.** DPS reserves the right to immediately suspend furnishing information covered by the terms of this agreement to User when any terms of this agreement are violated or reasonably appear to be violated. DPS shall resume furnishing such information upon receipt of satisfactory assurances that such violations did not occur or that such violations have been fully corrected or eliminated. In the case that User challenges the ruling of DPS regarding violation(s) or audit results, the Comprehensive Data Systems Policy Board shall adjudicate the matter.
 - C. **Indemnification.** User hereby agrees to indemnify and save harmless DPS, its Director and employees, and the Federal Bureau of Investigation, its Director and employees from and against any and all claims, demands, suits, and proceedings by others and against all liability to others for the use or misuse by the User of any information provided to User pursuant to this agreement.
6. **Executory Clause.** It is understood by and between the parties hereto that DPS is obligated to provide the services described in Section 7 above to User only to the extent that public funds are made available to DPS for that purpose. DPS shall incur no liability on account thereof beyond the money made available for such purpose.
7. **Construction.** This agreement shall be liberally construed to apply to both manual and automated information systems wherever and whenever possible.

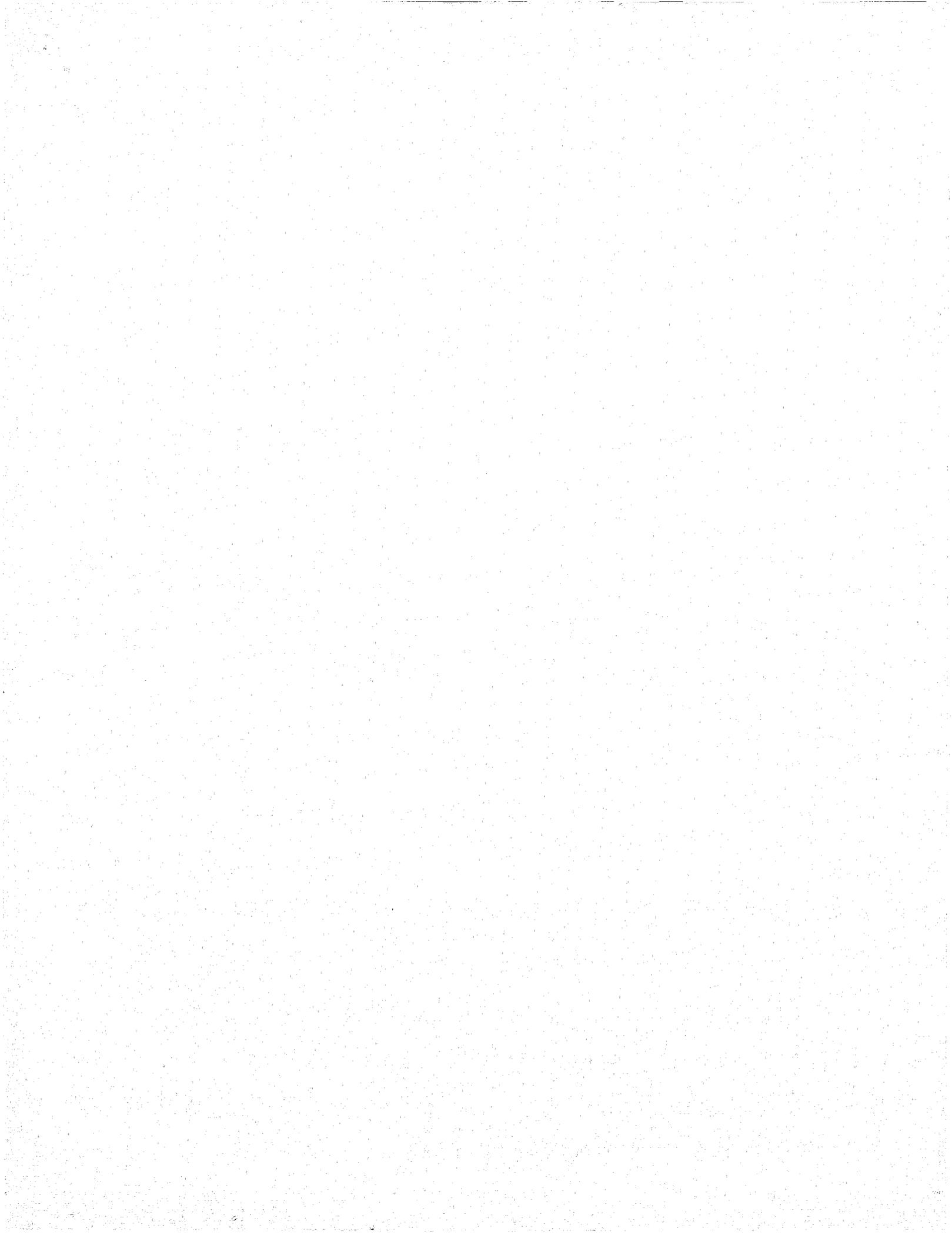
IN WITNESS WHEREOF, the parties hereto have caused this agreement to be executed by the proper officers and officials.

ARIZONA DEPARTMENT OF PUBLIC SAFETY

BY: _____
 TITLE: DIRECTOR _____
 DATE: _____

USER: _____

BY: _____
 TITLE: _____
 DATE: _____



CONTINUED

1 OF 2

ARIZONA REVISED STATUTES

§ 41-2201. Definitions

In this chapter, unless the context otherwise requires:

1. "§Board" means the comprehensive data system policy board.
2. "Center" means the criminal justice statistical analysis center, an operating section within the Arizona state justice planning agency.
3. "Component information system" means an independent information system serving one or more criminal justice agencies and which may participate in the criminal justice information system.
4. "Criminal history record information" means data collected on individuals by criminal justice agencies which consists of identifiable descriptions and notations of arrest, detentions, indictments, criminal informations or other formal criminal charges and any disposition arising therefrom, including sentencing, correctional supervision and release. Criminal history record information does not mean identification information, such as fingerprint records, to the extent such information does not indicate involvement of the individual in the criminal justice system, information associated with the administrative functions or correctional treatment process of a criminal justice agency or juvenile justice information.
5. "Criminal justice agency" means any court or government agency or division of such agency which performs the administration of criminal justice pursuant to statutory authority or executive order and which allocates a substantial part of its budget to the administration of criminal justice.
6. "Manager" means criminal justice information system manager.
7. "System" means criminal justice information system.

§ 41-2202. Comprehensive data systems policy board; term; compensation

A. There shall be a comprehensive data systems policy board consisting of twenty-one members for the purpose of administering and managing the Arizona criminal justice information system. Of the members first appointed, four shall be appointed for a term of one year and five members each for a term of two years. A member may be reappointed. Upon the expiration of any term of an appointed member, a successor shall be appointed for a full term of two years which shall expire on the third Monday in January of the appropriate year. Appointment to fill a vacancy caused otherwise than by expiration of a term shall be for the unexpired portion of such term. The board shall consist of the following members:

1. The director of the department of public safety.
2. The director of the department of corrections.
3. A justice of the Arizona supreme court appointed by the chief justice.
4. The presiding judge of the Maricopa county superior court.
5. The presiding judge of the Pima county superior court.

6. The sheriff of Maricopa county.
7. The sheriff of Pima county.
8. A member appointed by the Arizona chief probation officers' association.
9. The chief of police of Phoenix.
10. The chief of police of Tucson.
11. The chief adult probation officer of Maricopa county.
12. The chief adult probation officer of Pima county.
13. The county attorney of Maricopa county.
14. The county attorney of Pima county.
15. A state senator appointed by the president of the senate.
16. A state representative appointed by the speaker of the house.
17. Two lay members appointed by the governor to represent the public, neither of whom is employed by a criminal justice agency or holds an elected or appointed public office.
18. A member appointed by the Arizona police chiefs association.
19. A member appointed by the Arizona association of county attorneys.
20. A member appointed by the Arizona association of county sheriffs.

B. The governor shall appoint a member to be chairman for a term of one year. A chairman may be reappointed.

C. The members shall receive no compensation but shall be entitled to reimbursement for expenses in accordance with the provisions of title 38, chapter 4, article 2.¹

§ 41-2203. Powers and duties of the board

- A. The board shall:
1. Establish the technical criteria to be followed for connecting a component information system to the system.
 2. Adopt bylaws for the administration of the board.
 3. Adopt and promulgate rules and regulations for the administration and management of the system.
 4. Conduct hearings to adjudicate disputes between criminal justice agencies if the dispute concerns lack of compliance by either of such agencies with rules and regulations promulgated by the board.

5. Receive petitions for review of criminal history record information from the subject of such information, conduct hearings to determine the accuracy of the information concerning the subject and amend such criminal history record information if inaccurate.

6. Formulate policies, plans and programs for expansion of the system as needed.

7. Set developmental priorities for the system.

8. Develop and submit to the legislature cost sharing formula for participants in the system.

9. Advise and make recommendations to the governor, legislature, judiciary and local governments on matters concerning the objectives of the board.

10. Make an annual report on the operation of the board.

11. Provide information to the public on the purposes of the system.

12. Adopt and promulgate rules and regulations for the privacy, confidentiality and security of the system and the dissemination of criminal history record information.

13. Set policy, establish guidelines, and oversee the collection, analysis and publication of statewide criminal justice data and statistics by the center.

14. Review research studies and reports produced by the center prior to the publication of such studies and reports.

15. Adopt plans for the implementation of the system and the privacy, security and confidentiality of criminal history record information.

B. The board may:

1. Establish joint research and information facilities with governmental and private agencies.

2. Accept and expend public and private grants of funds, gifts and contributions to effectuate the purposes of this chapter.

§ 41-2204. System manager; powers and duties

There shall be a system manager appointed by the board. The manager shall serve at the pleasure of and be responsible to the board. The manager is exempt from the provisions of the state personnel system and is eligible to receive compensation pursuant to § 38-611. The manager shall:

1. Execute the policies of the board and supervise the operations of the system.

2. Coordinate and standardize the design, development and implementation of the system and subsystem.

3. Provide for system and subsystem planning.

4. Enforce the rules and regulations relating to the security, privacy, confidentiality and dissemination of criminal history record information.

5. Submit recommendations to the board concerning establishment of research, statistical and planning programs including a study of the system.

6. Provide criminal justice agencies with criminal history record information for operational and management purposes in accordance with the rules and regulations established by the board governing the dissemination of such information.

7. Perform such other powers and duties as may be prescribed or delegated by the board.

§ 41-2205. Criminal justice information system central repository

A. There shall be a central repository for the collection, storage and dissemination of criminal history record information. The department of public safety shall operate the central repository pursuant to the rules and regulations adopted by the board. The department of public safety shall conduct annual audits to insure each criminal justice agency is complying with rules and regulations governing the maintenance and dissemination of criminal history record information.

B. Each criminal justice agency shall report criminal history record information, whether collected manually or by means of an automated system, to the central repository pursuant to the provisions of ARS 41-1750 and 41-1751.

§ 41-2206 Disciplinary action; system participants

Any agency, company or individual who fails to conform to the rules and regulations adopted pursuant to this chapter may be subject to removal from participation in the system by action of the board. Added Laws 1977, Ch. 131, § 2, eff. May 31, 1977.

¹Section ARS 38-621 et seq.



END