

STATE OF UTAH



CALVIN L. RAMPTON
Governor

CRIMINAL HISTORY PRIVACY AND SECURITY PLAN

JANUARY 1976

UTAH STATE DEPARTMENT OF PUBLIC SAFETY

RAYMOND A. JACKSON
COMMISSIONER

PREPARATION AND PRINTING OF
THIS DOCUMENT FINANCED BY
LAW ENFORCEMENT ASSISTANCE ADMINISTRATION
GRANT # 76-T.A-99-6024

43480

STATE OF UTAH



CALVIN L. RAMPTON
Governor

CRIMINAL HISTORY PRIVACY AND SECURITY PLAN

JANUARY 1976

UTAH STATE DEPARTMENT OF PUBLIC SAFETY

RAYMOND A. JACKSON
COMMISSIONER

PREPARATION AND PRINTING OF
THIS DOCUMENT FINANCED BY
LAW ENFORCEMENT ASSISTANCE ADMINISTRATION
GRANT # 76-T.A-99-6024



CALVIN L. RAMPTON
Governor

THE STATE OF UTAH

DEPARTMENT OF PUBLIC SAFETY
317 STATE OFFICE BUILDING
SALT LAKE CITY, UTAH 84114

RAYMOND A. JACKSON
Commissioner

January 2, 1976

Mr. Richard W. Velde, Administrator
Law Enforcement Assistance Administration
U. S. Department of Justice
633 Indiana Ave.
Washington, D.C. 20530

Dear Mr. Velde:

The State of Utah is pleased to present its Criminal History Privacy and Security Plan. This letter and its attachments fulfill the requirements of the May 20, 1975 Regulations issued by LEAA requiring the development of this Plan.

The State of Utah is especially supportive of the concepts of privacy and security and our State has taken several steps toward full compliance with the Regulations. As of the date of this letter, many of the features of our Plan are operational; and we have embarked upon an aggressive program to attempt to achieve full compliance with the Regulations on, or before, December 31, 1977. Furthermore, the State of Utah has implemented the procedures outlined in our Plan to the maximum extent feasible.

Because Utah recognizes the importance of protecting an individual's rights of privacy and security, we intend to implement the procedures contained in our Plan throughout the State in agencies not directly affected by the Regulations, as well as those agencies who must comply with the Regulations. This will not be a simple task. It will require a long-range effort to gain widespread support for the Plan and to demonstrate to these unaffected local agencies that they will benefit directly from implementation of the guidelines to be developed.

The State of Utah is confident that our Plan will meet the needs of privacy and security of criminal history record information, and we are hopeful that our Plan will meet with early LEAA approval.

Please feel free to contact me regarding any questions needing clarification.

Sincerely,

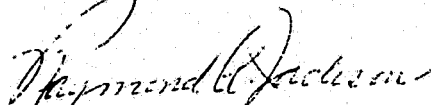

Raymond A. Jackson
Commissioner



TABLE OF CONTENTS

<u>SECTION</u>	<u>TITLE</u>	<u>PAGE</u>
	Transmittal Letter	
	Preface	
I	OBJECTIVES OF THE PLAN	1
	A. Completeness and Accuracy	2
	B. Limits on Dissemination	2
	C. Audits and Quality Control	3
	D. Security	3
	E. Individual Right of Access and Review	4
	F. Certifications	4
	G. Standards and Goals	5
II	APPROACH TO ACHIEVING THE OBJECTIVES	6
	A. Completeness and Accuracy	6
	1. State Central Repository	6
	2. Disposition Reporting	8
	a. Disposition Reporting Within 90 Days	10
	b. Promptness of Reporting and Delinquent Disposition Monitoring	12
	c. Disposition Reporting of Arrests Occurring After June 19, 1975	14
	3. Repository Query Before Dissemina- tion	15
	4. Maintaining Accuracy of Records	16
	5. Dissemination from Criminal History Record Systems Other than the Central Repository	18

TABLE OF CONTENTS

<u>SECTION</u>	<u>TITLE</u>	<u>PAGE</u>
II (Cont.)		
B.	Limits on Dissemination and Agencies Authorized	20
1.	General Policies on Use and Dissemination	21
2.	Sanctions for Individuals and Agencies	25
3.	Validating Agency Right of Access	26
4.	Notices to Agencies not Directly Subject to the Regulations	27
C.	Audits and Quality Control	28
1.	Systematic Audits	28
2.	Annual Audits/Compliance Reviews	30
D.	Security and Confidentiality	32
1.	Hardware and Software	32
a.	General Security Provisions	34
b.	Procedures for Access	36
c.	Dedication	36
2.	Management Control and Designation of the Responsible Agency	37
3.	Personnel	38
4.	Physical Security	39
E.	Individual Right of Access and Review	40
1.	Verification of Identity	41

TABLE OF CONTENTS

<u>SECTION</u>	<u>TITLE</u>	<u>PAGE</u>
II (Cont.)		
	2. Rules for Access	42
	3. Point of Review and Mechanism	42
	4. Challenge	44
	5. Administrative Review and Record Correction	45
	6. Appeal	46
	7. Correction	46
	8. Information Subject to Review	48
F.	Certification Statment	48
	1. Applicable Criminal Justice and Non-Criminal Justice Agencies	48
	2. Certification Checklist for the State Repository	52
	3. Certification Checklists for Other Agencies	53
	4. Legislation Dealing with Plan Compliance	54
	5. Other Legislation/Executive Orders for Non-Criminal Justice Users for Dissemination of Criminal History Data	54
	6. Progress toward Problem Resolution	55
G.	Relevant Statewide Criminal Justice System Standards and Goals	56
III	SCHEDULE OF MAJOR MILESTONES	57
IV	RESPONSIBILITIES OF INVOLVED AGENCIES	66

LIST OF EXHIBITS

PAGE

II	-	1:	Sample Notice	27
II	-	2:	Summary of Certification Applicability Criteria Determination Survey	49
III	-	1:	Action Plan and Schedule	59
IV	-	1:	Proposed Organization for Privacy and Security Plan Implementation, Operation and Maintenance	67
IV	-	2:	Statewide Plan Implementation Cost Estimate Development Details	70

APPENDICES

A.	LEAA Regulations
B.	Criminal Identification Statute: Title 77, Chapter 59, Utah Code Annotated 1953
C.	Utah Arrest and Court Disposition Report
D.	Sample User Agreements
E.	Juvenile Records Dissemination Exceptions
F.	Agencies Authorized Access to Criminal History Record Information
G.	Computer Security Guidelines for Implementing the Privacy Act of 1974
H.	Applicable Agency List/Certification Process Requirement Checklists
I.	Applicability Criteria for Certification Determination
J.	Certification Applicability Criteria Determina- tion Survey Forms
K.	Master Certification Elements

- L. Certification Procedure
- M. Criminal Justice System Standards and Goals
- N. State Central Repository Certification Checklist
- O. Certification Checklists for Other Agencies

PREFACE

In recognition of the impact the Criminal History Privacy and Security Plan would have upon the criminal justice system throughout the State of Utah, the Criminal History Privacy and Security Committee appointed a selected Task Force of representatives from all sectors of the criminal justice community to participate in the actual preparation of the Plan. This Criminal History Privacy and Security Task Force, working with the Council on Criminal Justice Administration, actively participated in writing the Plan. Mr. Corydon D. Hurtado, a systems planning consultant and President of Cyberserv International Co. also contributed to the development and preparation of the Plan.

Utah's Criminal History Privacy and Security Plan is an important step forward in fulfilling State and Federal goals of providing for the security and confidentiality of criminal history record information. Recognition should be afforded to all those who have contributed to the development of this significant document.

CRIMINAL HISTORY PRIVACY AND SECURITY COMMITTEE MEMBERS

Robert B. Andersen, Chairman
Utah Council on Criminal Justice Administration

Raymond A. Jackson, Commissioner
Utah State Department of Public Safety

David S. Young, Director
State Wide Association of Prosecutors

Wayne D. Shepherd, President
Utah Chiefs of Police Association

Dr. H. Roy Curtin, Acting Director
State Information System Center

Leo L. Memmott, State Legislative Budget Analyst
Office of Legislative Research

Arthur G. Christean, Deputy State Court Admin.
Office of Court Administrator

Sheriff Floyd Witt, President
Utah Sheriff's Association

Ernest Wright, Director
Division of Corrections

Ivard Rogers, Director
Utah Bureau of Identification

Robert Hansen, Deputy Attorney General
Utah Attorney General's Office

John McNamara, Administrator
Utah Juvenile Court

Commissioner Harold Smith, Representative
Governor's Advisory Council on Community Affairs

Leon Sorenson, Director
Office of Legislative Research

Ned Wilson
Office of Lieutenant Governor

CRIMINAL HISTORY PRIVACY AND SECURITY TASK FORCE MEMBERS

Jim Mills, Data Processing Coordinator
Utah State Department of Public Safety

Earl F. Dorius, Assistant Attorney General
Utah Attorney General's Office

Fred Schwendiman, Administrative Assistant
Department of Public Safety

Mike Phillips, Deputy Administrator
Utah Juvenile Court

Dr. H. Roy Curtin, Acting Director
State Information System Center

Kent Nielsen, Systems Analyst
State Information System Center

Wayne D. Shepherd, President
Utah Chiefs of Police Association

Art Christean, Deputy State Court Administrator
Office of Court Administrator

Richard Strong, Analyst
Office of Legislative Research

Gene A. Roberts, Manager
Utah Council on Criminal Justice Administration

Richard Horlocher, Criminal Identification Specialist
Utah Bureau of Identification

Robert White, Criminal Identification Specialist
Utah Bureau of Identification

Arthur J. Hudachko, Information Systems Program
Coordinator
Utah Council on Criminal Justice Administration

I. OBJECTIVES OF THE PLAN

On May 29, 1975 LEAA issued Regulations requiring the development of a Criminal History Record Information Plan, setting forth operational procedures to provide for the privacy and security of such records. It is the intent of the State of Utah to fulfill the requirements of LEAA's Regulations through the development and implementation of this Criminal History Record Information Privacy and Security Plan (Plan). A copy of the Regulations is contained in Appendix A.

The authority for these Regulations is derived from Section 524(b) of the Omnibus Crime Control and Safe Streets Act (P.L. 93-83) which provides:

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

To implement these Regulations, the Governor has instructed the Commissioner of the Department of Public Safety to proceed with the development and implementation of a plan which sets

forth operational procedures on: (a) completeness and accuracy, (b) limits on dissemination, (c) audits and quality control, (d) security and confidentiality and (e) individual right of access and review. The balance of this section describes the objectives in each major operational procedure area.

A. Completeness and Accuracy

The objective of the Plan's completeness and accuracy procedures is to ensure that criminal history record information is complete and accurate. "Complete" means, in general, that arrest records should indicate all subsequent dispositions as the case moves through the various segments of the criminal justice system. "Accurate" means containing no erroneous information of a material nature.

To fulfill this objective, the State of Utah will continue to operate its Central Repository, the Utah Bureau of Identification (UBI), and to refine the overall UBI capabilities and organizational framework. The Plan outlines procedures which provide for prompt reporting of disposition data to UBI and establishes a mechanism whereby criminal justice agencies can query the Central Repository prior to dissemination of any criminal history record information to assure that the most current disposition data is being utilized. Formal user agreements will be executed between the Central Repository and its users and between other criminal justice agencies and their third party users. Operational procedures are established within the Plan to minimize the possibility of a criminal justice agency's recording and storing inaccurate information and implementation of a system for notification of prior recipients upon discovering erroneous criminal history information.

B. Limits on Dissemination

The objective of the Plan's procedures for limiting dissemination of criminal history record information is to be responsive to the requirements of Section 524(b) of the Safe Streets Act requiring that dissemination and use of criminal history information be limited to "criminal justice and other lawful purposes."

The Plan sets forth procedures currently operational or planned to become operational relating to dissemination for criminal

justice purposes such as licensing, employment checks, security clearances and research. The Plan sets restrictions and limitations on juvenile record dissemination and secondary dissemination by non-criminal justice agencies. Procedures are indicated relative to validating an agency's right to access information and expiration of information availability. The Plan includes Criminal History Record Information User Agreements for all State and local criminal justice agencies subject to the Regulations and a "notice" to agencies not directly subject to the Regulations indicating the imposition of sanctions for information misuse and specifying restrictions on dissemination and internal agency use.

C. Audits and Quality Control

Audits and quality control procedures are necessary to determine the extent that criminal justice agencies are complying with the Plan's components. The objective for the audit and quality control procedures is to monitor for compliance.

The Plan indicates two different forms of auditing. Systematic audits will be utilized as a quality control mechanism and will provide a means of guaranteeing the completeness and accuracy of criminal history record information. Annual compliance reviews (audits) will provide an examination of a representative sample of State and local criminal justice agencies chosen on a random basis to verify adherence to the Plan's provisions and will specifically identify documents and data elements to be maintained to support this process.

The Plan describes in detail both types of audits and identifies procedures and the organizational approach to be used in fulfilling this objective.

D. Security and Confidentiality

The objective of these procedures is to provide adequate safeguards over the security and privacy (confidentiality) of criminal history record information. The Plan sets forth procedures relative to: effective hardware and software design to prevent unauthorized access; management control capabilities; personnel requirements; and physical security.

For purposes of understanding the concept of privacy and security as used in this Plan, it is necessary to define security and confidentiality.

- . Security refers to the physical protection of data, information, records, equipment, and facilities from accidental or intentional (but unauthorized) modification, destruction or disclosure.
- . Confidentiality (privacy) is a concept which applies to data. It is the status accorded to data which requires controls over dissemination which are strictly a function of the integrity of the people with access to criminal history record information and the controls exercised to prevent unauthorized disclosure and use of the information.

Another way to view the concept of a privacy and security plan is to think of confidentiality as the ultimate objective of such a plan. Security is then viewed as the measures of protection which are implemented at specified levels to achieve a pre-determined degree of confidentiality.

E. Individual Right of Access and Review

Section 524(b) of the Safe Streets Act guarantees the right of an individual to review information maintained about them and to permit the individual to challenge and correct such information if they deem it to be inaccurate and incomplete. The objective of these procedures is to allow an individual to execute this right of law.

The Plan sets forth procedures for verification of identity, access and review, challenge, administrative review and record correction, appeals and notification to prior recipients of corrected information. These procedures, to become completely operational Statewide by March 16, 1975, will achieve this objective.

F. Certifications

The State Plan includes a certification stating the extent to which Plan procedures have been implemented and details the steps undertaken to achieve full compliance. The objective of the annual certification process is to determine when the State is in full compliance with the Regulations.

The certification will consist of the following:

- . Applicable criminal justice and non-criminal justice agencies.
- . Checklist of operational procedures and compliance comment for the State Central Repository.

- . Checklist of operational procedures and compliance comment for other criminal justice agencies covered by the Regulations.
- . Legislation/Executive orders issued or pending related to Plan compliance.
- . Legislation/Executive orders authorizing dissemination of criminal history data to non-criminal justice agencies.
- . Narrative discussion of progress toward problem resolution to achieve complete and accurate criminal history information.

The certification provides that all procedures in the State Plan will be fully operational and implemented by December 31, 1977. Certification will be submitted in December of each year to LEAA until such complete compliance is achieved. The yearly certifications will update the information provided under Section 20:21 of the Regulations.

G. Standards and Goals

The State has adopted formal criminal justice system standards and goals. LEAA established recommended guidelines for criminal justice systems standards and goals to be implemented nationwide. In developing its standards and goals, Utah followed these recommended guidelines and modified them as required to fit the State's needs.

The Regulations do not address the subject of these nationally coordinated and developed standards. However, the State believes that portions of this State's standards and goals dealing with privacy and security should be integrated with the Plan's implementation. The objective of this segment of the Plan is to fulfill this implementation need.

II. APPROACH TO ACHIEVING THE OBJECTIVES

This section presents the current and proposed operating procedures the State of Utah intends to employ in order to meet the objectives and requirements of the May 20, 1975 LEAA Regulations. Procedures which are presently operational are described. All proposed procedures take into consideration the extent to which currently operational procedures can become a part of the proposed procedures.

A. Procedures to Achieve Completeness and Accuracy

Section 20:21(a) of the Regulations requires the implementation of procedures to ensure that criminal history record information is complete and accurate. The Regulations suggest the best method would be to establish a central State repository for all criminal history record information. The Regulations also require the establishment of a disposition reporting system and record query procedures.

1. State Central Repository

LEAA Regulations Requirements: The Regulations do not strictly mandate the establishment of a State central repository. This approach is suggested as the most effective, efficient and economical way to satisfy the overall need for completeness and accuracy of criminal history record information.

Present Procedures: The State of Utah has a State Central Repository of criminal history records to serve all criminal justice agencies. Its organization and functions are outlined in the Utah Code Annotated 1953, Title 77, Chapter 59 (see Appendix B). The Utah Bureau of Identification (UBI) is part of the Department of Public Safety, and UBI serves as the State Central Repository. UBI began its initial operations April 1, 1927 by an act of the State Legislature.

To enable UBI to maintain files of criminal history records for the State, the Statute provides the following:

- . All police and sheriff departments in the State shall transmit to UBI and the FBI, fingerprints and related data about all persons

arrested on criminal charges. Penal institutions are also required to transmit fingerprints and related data concerning all commitments and also to furnish release information.

- . Criminal justice agencies are given the authority and duty to take, or cause to be taken, fingerprints, photographs and other descriptive data of offenders coming under their jurisdiction.
- . All court clerks or judges are required to forward dispositions of criminal cases to UBI.

The Statute further provides that information pertaining to the identification and history of an individual on file shall be released, upon application, to criminal justice agencies and other bureaus similar in nature in any state in the United States or in any jurisdiction thereof, or in any foreign country. The Statute also provides that only UBI employees and persons specifically authorized by the Commissioner of Public Safety shall have access to the files or records of UBI and that no file or record shall be disclosed by any employee except to authorized agencies. Any person who willfully gives false information or withholds information in any report or who shall remove, destroy, alter or mutilate any file or record of UBI shall be guilty of a misdemeanor.

UBI is currently staffed with 20 employees funded by State appropriations and with 5 employees funded with LEAA funds. Work is divided into the following sections: Fingerprint, Records and Coding, Communication, and Criminal Intelligence. The Communication Section operates 24 hours-a-day, 7 days-a-week and serves as the State control terminal for law enforcement agencies using the National Crime Information Center and relay center for the Utah Law Enforcement Teletype Network and the National Law Enforcement Telecommunications System.

UBI has a manual file of approximately 250,000 criminal records of persons who have been arrested throughout Utah dating back to the 1920's. Since November 1972 all arrest records received from contributors have been computerized. Over 45,000 summary records are on-line

for terminal access. Currently, 13 criminal justice agencies have terminal access to these records; most serve as area dispatch centers. Agencies having no terminal access contact their area dispatch center which makes the inquiry for them.

Proposed Procedures: Because the State currently has a fully operational central repository for criminal history record information, no new procedures or legislative action are required.

2. Disposition Reporting

LEAA Regulations Requirements: The Regulations require the establishment of a disposition reporting system and require such a system to maintain complete dispositions by every component of the criminal justice system (police, prosecutors, courts and corrections). The Regulations also require that dispositions occurring within the State must be reported within 90 days after the disposition has occurred. LEAA has interpreted the Regulations' requirements for a disposition reporting system to include provisions for monitoring delinquent dispositions.

Present Procedures: The State currently has a disposition reporting system under development, but no procedures have been implemented. However, several agencies are presently reporting dispositions to the State Central Repository.

Proposed Procedures: The need for comprehensive disposition reporting in the State of Utah has long been recognized as essential. Improvement is needed in collecting and reporting disposition data. Presently about 30 percent of all dispositions are reported to the State Central Repository. Many problems exist in the present reporting methods of agencies currently reporting dispositions to the Central Repository and there are some agencies not yet attempting to report dispositions.

One of the major problems existing today is that disposition data reported by each agency on the same individual is difficult to tie back to that individual. Charges and even names are changed as a defendant is processed through the criminal justice system, making utilization by the State Bureau of Identification impossible.

The proposed disposition reporting system will give the needed improvement. The vehicle to be used for reporting dispositions is the Utah Arrest and Court Disposition Report (UACDR). This form (see Appendix C) is initiated by the appropriate agency when the individual defendant enters the Utah Criminal Justice System. As the individual progresses through the police, prosecutor, courts and correctional agencies, disposition data will be initiated and reported to the Central Repository via the UACDR form.

During the past year, a Federally funded effort has been underway in the State to establish an Offender Based Transaction Statistics System (OBTS). The approach to this project has been a two phase effort: Phase 1 is disposition reporting; and Phase 2 is statistical data reporting. The disposition reporting portion of the OBTS system is the disposition reporting system outlined herein. However, the system outlined is a proposed system and has not been implemented anywhere in the State.

The Disposition Reporting System as proposed has several basic objectives which include the capability to:

- . Collect final disposition information from police, prosecutor, trial courts, appellate courts, correctional institutions and probation and parole agencies.
- . Comply with 90-day reporting requirements.
- . Establish disposition control and monitoring procedures.
- . Collect information necessary to complete arrest data on criminal histories for rap sheets and other statistical type data.
- . Provide statistical data to other agencies to support at least five general areas: planning, budgeting, monitoring, evaluation and general research.

The basic legal authority, which establishes disposition reporting requirements for police, sheriff, court clerks, judges, justices of peace and correctional agencies to the State Central Repository, is

stated in the Utah Code Annotated 1953, Title 77, Chapter 59 (77-59-9, 77-59-11, 77-59-12, 77-59-13, 77-59-14). These Statute sections are presented in Appendix B.

a. Disposition Reporting Within 90 Days

Disposition reporting is being developed as an integral part of the Computerized Criminal History (CCH) and Offender Based Transaction Statistics (OBTS) system. The basic approach to disposition reporting is through the use of the pre-numbered three part UACDR form (see Appendix C). The form will be generated at the time a defendant is booked into a city or county jail.

The UACDR form is designed to follow the defendant through the criminal justice system from point of arrest to final court disposition. Each agency is responsible for reporting dispositions to UBI's Central Repository as soon as possible, or at least within 30 days of disposition. The form is designed to permit handwritten completion in order to aid reporting clerks to expedite disposition reporting.

Each UACDR form and all sections of the form have a preprinted Court Disposition Report number (CDR). This number serves as a control to tie together all actions that affect the identified defendant. The CDR number will be used by the computer master files as the major control for arrest and charge.

Dispositions reported to the Central Repository will be processed, checked and entered on the Computerized Criminal History master file via key tape data entry devices. The ability to receive computerized disposition reporting is another essential built-in phase of the disposition reporting system. Salt Lake City, Salt Lake County, Weber County and Utah County are presently in planning and development phases of automated disposition reporting systems.

Computer validation and conditional checks will be made on all disposition input. Errors will be flagged and displayed as they are found. Conditional checking will assure completeness, accuracy and consistency of input. Audit trails will be provided

to account for all transactions processed.

Field representatives from UBI will be available for training and personal contact with reporting agencies on a scheduled basis. Field representatives are key factors in the success of this reporting system. The primary duties of field representatives will be to:

- . Train reporting agency personnel in the use of UACDR forms.
- . Aid agencies in the solution of problem areas.
- . Audit reporting procedures and ensure accuracy.
- . Follow-up on delinquent dispositions.
- . Maintain control of reporting input.
- . Provide assurance that dispositions are being reported within the State's 30-day rule and LEAA's 90-day rule.

Standard procedures will be implemented throughout the Utah Criminal Justice System to ensure that dispositions are reported on a timely and accurate basis. These procedures are:

- . Police: The booking agency initiates the UACDR reporting process by completing the identification section and fingerprinting the defendant on the first page or fingerprint card portion of the form. The identification section is carboned through to the remaining copies of the form, which provides positive identification data to other users of the form.

The pre-numbered completed fingerprint card will be forwarded to the Central Repository by the booking agency. This will establish each defendant on the Central Repository's Computerized Criminal History master file along with initiating disposition control and delinquent disposition monitoring for each arrest and charge filed against a defendant.

The contributing law enforcement agency will forward the remaining copies of the UACDR form to the court before the defendant is to appear to answer for the specified charges.

- . Prosecutor, Trial Courts, Appellate Courts:
The next agency involved in the reporting process is either a justice of the peace or city clerk's office. The type of charge(s) and jurisdictional area are the determining factors. City clerks are responsible for completing the arraignment and preliminary hearing portion of the UACDR form. The completed sections will then be forwarded to the Central Repository for processing.

If the charge is a felony or an appeal, the UACDR form is forwarded to the county clerk for district court cases. County clerks will also be responsible for completing disposition information on cases where a conviction is appealed to the Supreme Court.

- . Corrections, Probation/Parole: At the time of sentencing, an official representative of the Division of Corrections will be present in court. The CDR number will be picked up at that time for inclusion in the system. Present disposition forms used by the Division of Corrections and Adult Probation and Parole will be utilized for reporting of disposition information to the Central Repository.

b. Promptness of Reporting and Delinquent Disposition Monitoring

The disposition reporting system will contain a delinquent disposition monitor program as an integral part of the system. The delinquent disposition monitor program will be created to flag all records where a predetermined time period has elapsed since the last reported disposition.

The delinquent disposition monitor will perform three basic monitoring functions:

- . UBI field representatives will be notified via a computer listing of all potentially

delinquent dispositions not yet reported to the Central Repository. The listing will be used to maintain control of the system and for input follow-up.

- . A criminal disposition inquiry notice will automatically be generated and sent to agencies holding delinquent dispositions.
- . An unreported disposition monitor will analyze each criminal history record contained on the Central Repository's master file. If charges do not contain disposition information, a flag will indicate the lack of dispositions to anyone trying to access the records.

Reports will be generated for use by UBI field representatives to control, monitor, audit and maintain the system. Statistical reports will also be generated to produce statistical information on:

- . How criminal justice operates in processing defendants and how agencies and functions relate to one another.
- . How much time it takes for the criminal justice system to process individuals.
- . Who the clients of the criminal justice system are.

Under the one-year rule relating to disposition monitoring, criminal history record information concerning the arrest of an individual may not be disseminated to a non-criminal justice agency or individual if an interval of one year has elapsed from the date of arrest and no disposition of the charge has been recorded, and no active prosecution of the charge is pending. This one-year rule does not apply in the following exceptional instances:

- . Individuals and agencies pursuant to a specific agreement with a criminal justice agency to provide criminal justice administration services (where the agreement sets forth certain use conditions and sanctions for usage violations).

- . Individuals and agencies pursuant to a specific agreement with a criminal justice agency for research, evaluative or statistical activities (where the agreement sets forth certain conditions and sanctions for usage violations).
- . State or Federal government agencies authorized by statute or executive order to conduct security clearance eligibility.
- . Individuals and agencies authorized by court order or court rule.

Terminal output flags will be employed and coded on the Central Repository's master file records to ensure that computer terminal operators throughout the State will not mistakenly release inaccurate information to unauthorized sources. Each criminal history record not having a disposition within one year of arrest will be flagged to alert the operator that certain segments of the criminal history record are subject to restricted dissemination.

The Regulations do not restrict the dissemination of criminal history information with potentially delinquent dispositions to criminal justice agencies. However, procedures will be implemented as part of the delinquent disposition monitor to alert these agencies of this potential inaccuracy.

c. Disposition Reporting of Arrests Occurring After June 19, 1975

On June 19, 1975 a Statewide disposition reporting system was not operational. This system is currently in the final design stage and will be operational by October 31, 1976. Until the system is operational, UBI staff will contact police, court, and correctional agencies where feasible to assist them in submitting dispositions in order that criminal history records can be updated.

Although no formal Statewide disposition reporting system is operational which provides for disposition reporting within 90 days after the disposition has occurred, UBI will collect dispositions on an interim basis. UBI will receive disposition data for all individuals who enter or exit the State

Prison. Also, some law enforcement agencies send UBI a copy of the FBI disposition report form. In both of these instances, UBI will match fingerprints and will update the appropriate Central Repository records. In addition, where individual instances arise of a need-to-know basis, UBI will follow up with criminal justice agencies to collect these individual dispositions for updating the appropriate Central Repository record. Through these interim procedures, it is estimated that approximately 50% of all dispositions will be recorded on the Central Repository's records.

When the new Statewide disposition reporting system becomes fully operational, UBI does not intend to research all criminal history records to update all prior dispositions which were not reported. However, in individual instances of a need-to-know nature, UBI will follow up with criminal justice agencies to collect these dispositions for updating the appropriate Central Repository record.

3. Repository Query Before Dissemination

LEAA Regulations Requirements: The Regulations require criminal justice agencies to query the State Central Repository before any criminal history record information is disseminated. The intent of LEAA is to assure that the most recent disposition data is being disseminated. In cases where no central repository exists (which is not the case for the State of Utah), the Regulations allow for certain exempt situations when a query before dissemination would not be required.

Present Procedures: No formal procedures, policies or statutes exist which compel a criminal justice agency to query the UBI State Central Repository. However, since Utah has an operational central repository and an on-line Statewide communications network, most criminal justice agencies use the State Central Repository as their primary source for obtaining current and accurate criminal history record information.

Proposed Procedures: The user agreement negotiated with each criminal justice agency will require them to query the State Central Repository prior to dissemination of criminal history records outside their own department in order that they may furnish up-to-date disposition data. Queries shall be made to the Central Repository except in the following situations:

- . The date of arrest and/or disposition is so recent that the Central Repository would not have had sufficient time to add it to their files.
- . If the disposition cannot be determined from the on-line summary file, and the off-line criminal history file is incapable of providing the information in less than eight hours, or when it is needed for arraignment or bail setting.
- . Time is of the essence, and the Central Repository is technologically incapable of responding within the necessary time period.

Sample user agreements are presented in Appendix D.

Maintaining Accuracy of Records

LEAA Regulations Requirements: The Regulations require criminal justice agencies to maintain accurate criminal history records. While this accuracy requirement is related to the disposition reporting function (e.g. the one-year rule, terminal output flags, 90-day reporting of dispositions, etc.), it mainly relates to the quality of all information kept on file. The Regulations suggest that criminal justice agencies institute procedures of data collection, entry, storage and system audit to minimize the possibility of recording and storing inaccurate information. Also, when inaccurate information is discovered, all criminal justice agency recipients of the inaccurate information shall be notified.

Present Procedures: Normal input data audit checks and computer data validation routines are applied to each input and output process for the computerized criminal history record information files of the

State Central Repository. However, it is difficult, if not impossible, to determine the extent that acceptable data audit checks and validations are employed by criminal justice agencies throughout the State. No formal procedures, policies or statutes exist which require the use of some standard data audit procedures by local criminal justice agencies.

Proposed Procedures: All criminal history information received by the State Central Repository from contributors will continue to be checked for completeness and accuracy. If any obvious errors are noted or any information is lacking, the contributing agency will be contacted with a request to provide the correct data. The identification and arrest segments from incoming fingerprint cards will then be prepared for computer input and will be processed through computer data audit routines.

Data input staff will ensure through verification that all data elements necessary to create or update the computerized record are complete and accurate. All data elements will be edited by the computer data validation routines to ensure that all requirements for input are met. All errors noted will be corrected and re-entered.

In criminal justice agencies that do not have an automated system, all arrest records will be manually checked and verified for completeness and accuracy. If any obvious errors are noted or any information is lacking, the appropriate individual within the agency will be contacted with the request to provide the necessary information.

The accuracy of automated disposition information will be ensured by two methods :

- . Visual screening of disposition input will take place before input data can be entered for computer processing. Discrepancies will be resolved, and the audited documents will then be processed through the system.
- . Computer validation and conditional checks will be made on all data elements either individually or as a part of conditional

checking. All elements validated will be checked for format, limit and correctness.

Disposition errors will be flagged and displayed as they are found.

Typical input data audit checks and computer data validation routines will require that alpha fields contain A-Z or space, numeric fields contain numeric characters, date fields contain valid dates and coded fields contain valid codes. Conditional checks will assure completeness and consistency.

When it is determined that inaccurate information appeared on a criminal history record that has been distributed, reference will be made to the dissemination log to determine who has received copies of the erroneous information. These agencies will be notified and furnished a correct copy of the record. Upon furnishing a corrected copy, the dissemination log will be updated to indicate what correction information was sent and the date. Upon request, an individual whose record has been corrected shall be given the name of all non-criminal justice agencies to whom the record has been given.

5. Dissemination from Criminal History Record Systems Other than the State Central Repository

LEAA Regulations Requirements: The Regulations apply to any agency which maintains and disseminates criminal history records. In these instances such an agency is clearly subject to Section 524(b) of the Safe Streets Act and consequently, to the general requirement in the Regulations dealing with completeness and accuracy and disposition reporting.

Present Procedures: Presently, various criminal justice agencies maintain and disseminate criminal history record information from their own internally-developed systems. Some agencies have implemented disposition reporting systems in an attempt to maintain accuracy and completeness of the information.

However, this process is often times fragmented within the system in that procedures have not been developed to provide complete and comprehensive dispositional reporting at each interim stage in the criminal justice process. Only a small percentage of these dispositions are ever reported to the State Central Repository, and problems exist in present reporting methods of those agencies currently reporting.

Proposed Procedures: The implementation of a State-wide disposition reporting system will provide the necessary mechanism for local criminal justice agencies to maintain complete and accurate criminal history record information. Through the Utah Arrest and Court Disposition Reporting system, each agency is responsible for reporting dispositions to UBI's Central Repository no later than 30 days following the disposition. Dispositions reported to UBI will be processed, checked and entered on the computerized criminal history master file via key tape data entry devices. Computer validation and conditional checks will be made on all disposition input. Errors will be flagged and displayed as they are located. Conditional checking will assure completeness, accuracy and consistency of input. Terminal output flags will be utilized on UBI's master file records to ensure that computer terminal operators throughout the State will not release inaccurate or incomplete information. Procedures previously identified relating to restricted dissemination and delinquent disposition monitoring will also be in effect.

Manual file screening procedures consistent with the Central Repository will be implemented in criminal justice agencies where computerized systems are not in use. These procedures will be implemented to ensure that restricted criminal history information maintained on a manual system is not mistakenly released to unauthorized sources. The persons responsible for retrieval and dissemination shall visually screen each record to check each arrest that does not have a disposition and to see if one year has elapsed from the date of arrest and the current date. If one year has elapsed, then that segment of the record shall be updated to indicate that it is subject to restricted dissemination. The update will consist of an indicator such as a check mark (✓).

User agreements negotiated with each agency will require them to query the State Central Repository prior to dissemination of criminal history records outside their own department in order that they may furnish up-to-date disposition data. Agencies disseminating criminal history record information will be subject to the sanctions stipulated in the user agreement.

Designation of individuals responsible for obtaining dispositions and those in other agencies responsible for reporting dispositions will be identified at the time the user agreement(s) is exercised between agencies.

B. Limits on Dissemination and Agencies Authorized

Sections 20:21 (b), (c) and (d) of the Regulations establish limits for dissemination of criminal history record information. Criminal history record information may only be disseminated to the following authorized agencies:

- . Criminal justice agencies (for certain specified uses).
- . Other individuals and agencies which require criminal history record information to implement a statute or executive order referring to criminal conduct.
- . Individuals and agencies pursuant to a specific agreement with a criminal justice agency to provide criminal justice administration services (where the agreement sets forth certain use conditions and sanctions for usage violations).
- . Individuals and agencies pursuant to a specific agreement with a criminal justice agency for research, evaluative or statistical activities (where the agreement sets forth certain conditions and sanctions for usage violations).
- . State or Federal government agencies authorized by statute or executive order to conduct security clearance investigations to determine employment suitability or security clearance eligibility.
- . Individuals and agencies authorized by court order or court rule.

LEAA identifies the importance of these limitations in fulfilling the mandate of Section 524(b) of the Omnibus Crime Control and Safe Streets Act (P.L. 93-83) to ensure the privacy of information and to ensure that information is used only for law enforcement and criminal justice purposes.

Section 20:21(d) prohibits dissemination of juvenile records to non-criminal justice agencies under most situations, except where specifically allowed under Section 20:21(b) (3,4,6). Section 20:21(c) prohibits the dissemination of criminal history record information about an individual's arrest to non-criminal justice agencies under the one-year rule, except where specifically allowed under Section 20:21(b) (3,4,5,6).

1. General Policies on Use and Dissemination

LEAA Regulations Requirements: The Regulations establish restrictions on the use and dissemination of criminal history record information. This information may not be disseminated to a non-criminal justice agency or individual if one year has elapsed from the date of arrest and no disposition has been reported (one-year rule) or no prosecution is pending. Use of criminal history information disseminated to non-criminal justice agencies is limited to specified purposes and may not be disseminated further. Confirmation of the mere existence or non-existence of criminal history records is prohibited except under certain sections of the Regulations.

Present Procedures: Existing State statutes (see Appendix B) limit the dissemination of criminal history record information by UBI to criminal justice agencies and certain other authorized agencies. Any such dissemination must be based upon approval by UBI of an application. The Statute authorizes access to UBI files and records only by UBI employees and persons authorized by the Commissioner of Public Safety. The present categories of individuals and agencies authorized (police, prosecuting attorneys, judges, and officers of similar bureaus in other states or countries) are not the same as the categories prescribed in the Regulations.

Although the existing statutes meet present requirements, they are not fully responsive to the Regulations' requirements in that they deal only with dissemination by UBI and do not limit dissemination by other criminal justice agencies. However, most criminal justice

agencies in the State use some informal (and in some cases formal) process to restrict and limit dissemination.

Proposed Procedures: In the case of individuals and agencies acting pursuant to a user agreement with a criminal justice agency, the user agreement specifically identifies privacy and security terms and conditions. The user agreement authorizes access to data, limits the use of data to the purposes for which it was given, ensures the confidentiality and security of the data consistent with Federal regulations, limits liability of the State and its criminal history record information system, provides for renewal of the agreement at the end of each three-year period, provides for the destruction of disseminated information and copies thereof once the information is no longer needed for the purposes for which it was disseminated, and provides sanctions for violations thereof.

A user agreement will be executed between every criminal justice agency in the State and UBI. This process will allow free dissemination of criminal history record information among all criminal justice agencies without the use of additional agreements. Criminal justice agencies disseminating criminal history record information to non-criminal justice agencies will exercise a secondary user agreement (as needed). Both of these user agreements will be responsive to the provisions previously identified. A copy of both agreements with their specific provisions is presented in Appendix D.

Several general policies with respect to limits on dissemination are incorporated in this Plan. Criminal history record information concerning the arrest of an individual will only be disseminated to the following agencies (as stipulated in the Regulations):

- . Criminal justice agencies (for certain specified uses).
- . Other individuals and agencies which require criminal history record information to implement a statute or executive order referring to criminal conduct.
- . Individuals and agencies pursuant to a specific agreement with a criminal justice agency to provide

criminal justice administration services (where the agreement sets forth certain use conditions and sanctions for usage violations).

- . Individuals and agencies pursuant to a specific agreement with a criminal justice agency for research, evaluative, or statistical activities (where the agreement sets forth certain conditions and sanctions for usage violations).
- . State or Federal government agencies authorized by statute or executive order to conduct security clearance investigations to determine employment suitability or security clearance eligibility.
- . Individuals and agencies authorized by court order or court rule.

Also, criminal history record information will not be disseminated to a non-criminal justice agency or individual if an interval of one year has elapsed from the date of the arrest, and no disposition of the charge has been recorded, and no active prosecution of the charge is pending (except where dissemination is allowed under Section 20:21(b) (3,4,5,6) of the Regulations.

Procedures will also apply to three operational areas which are: juvenile record dissemination; confirmation of record existence; and secondary dissemination by non-criminal justice agencies. The following paragraphs describe these procedures:

- . Juvenile record dissemination: For internal uses of juvenile records, each file checked out to authorized persons will be recorded on a permanent file disbursement record card maintained in the file and removed only when checked out. The record card will be placed in an alphabetical file during the time the file itself is checked out. The alphabetical listing of checked out files will be reviewed periodically to locate files checked out for extensive periods. Only the central records point of a court office may disburse information to non-court personnel.

No information shall be provided any person unless he is properly identified as eligible.

No copies of any portion of the court record or probation officer records will be made without written permission of the clerk of the court except as otherwise provided in the procedures. A record of all copies made of original documents will be made on the file disbursement record card maintained with the file.

External dissemination of juvenile records will be restricted to certain agencies and individuals who have been properly identified as being eligible. No information will be provided without a written release from, or on behalf of, the juveniles involved (except in the circumstances outlined in Appendix E).

All court and probation officer records will be kept in a secure, restricted area of each Juvenile Court office maintaining such records. This area will be limited to access by authorized staff only as determined by the court clerk. The area, including computer terminals, will be locked when authorized staff are not in the restricted area. Files checked out to authorized staff are their responsibility and must be kept secure and away from public view when in use. No original court or probation officer records are to leave the court area except with a judge holding hearings at another location. Authorized copies of court or probation officer records must be maintained secure by the receiving person or agency and under no circumstances are to be re-disseminated without written authorization of the court.

- . Confirmation of record existence: No agency or individual in any criminal justice agency in the State will be authorized to confirm the existence or non-existence of criminal history record information for employment or licensing checks except in the following exceptional instances:

- . Criminal justice agencies (for certain specified users).
- . Other individuals and agencies which require criminal history record information to implement a statute or executive order referring to criminal conduct.

- . State or Federal government agencies authorized by statute or executive order to conduct security clearance investigations to determine employment suitability or security clearance eligibility.
- . Secondary dissemination by non-criminal justice agencies: Secondary dissemination of criminal history record information provided to non-criminal justice agencies will not be authorized. The use of criminal history record information disseminated to non-criminal justice agencies will be limited by the user agreement to the purposes for which it was given and shall not be disseminated further.

2. Sanctions for Individuals and Agencies

LEAA Regulations Requirements: The Regulations require that the Plan provide sanctions for violations in the use and dissemination of criminal history record information. These sanctions may be applied through legislation, contractual agreements or other appropriate methods. The intent of this requirement is to exercise control over all recipients of criminal history record information, whether or not they fall under the Regulations.

Present Procedures: Existing State Statutes (see Appendix B) provide sanctions for persons who willfully give false information, withhold information, or mishandle any records maintained by UBI. Such sanction is a misdemeanor. However, formal sanctions do not exist which are responsive to all elements of the Regulations.

Proposed Procedures: All individuals and agencies who are likely to receive disseminated criminal history information, even if not directly subject to the Regulations, shall be made aware of the Regulations prohibiting unauthorized disclosure through the notification procedure. In addition to the notification process describing sanctions for unauthorized disclosure, sanctions will be stipulated in the user agreement. The State will enforce strict compliance with the privacy and security requirements of the Regulations by requiring all criminal justice agencies directly subject to the Regulations to sign and comply with the terms of the user agreement. Upon violation of any rule, policy or procedure by authorized individuals or

agencies, the disseminating agency will immediately suspend furnishing any and all criminal history record information. Only upon receipt of satisfactory assurances that such violation did not occur or was corrected, will the disseminating agency reinstate the furnishing of criminal history record information. User agencies and individuals will also be subject to a misdemeanor and/or a fine for knowingly violating the terms of the user agreement. It should be noted that the sanctions of misdemeanor and/or fine are subject to legislative approval through the introduction of appropriate legislation.

3. Validating Agency Right of Access

LEAA Regulations Requirements: No specific reference to validation of agency right of access is contained in the Regulations. However, Section 20:21(b) of the Regulations does establish limits for dissemination of criminal history record information to specific authorized agencies. Consequently, before any dissemination is allowed, the potential recipient must be authorized under the Regulations to receive the information, and the disseminating agency must validate this right of access.

Present Procedures: No procedures are currently operational. However, each criminal justice agency determines when an agency is authorized access to specific criminal history records.

Proposed Procedures: When an agency requests information and claims to be authorized to receive such information pursuant to a statute, executive order or court order or rule, the disseminating agency will review the basis of such authority prior to dissemination.

The user agreements will also be used as a basis for determining right of access. If an individual or agency requesting criminal history information is not authorized by statute or by a user agreement, access will be denied.

Present authorized agencies are listed in Appendix F, as determined through researching the Utah Code. When the agency requesting information is not listed as an authorized agency the disseminating agency will refuse to release information pending receipt of an opinion from the Utah State Attorney General's Office after its coordination with the LEAA Office of General Counsel.

4. Notices to Agencies not Directly Subject to the Regulations

LEAA Regulations Requirements: Although the Regulations

EXHIBIT II-1 : SAMPLE NOTICE

The State of Utah has, with a combined effort of all criminal justice agencies throughout the State, prepared a comprehensive Privacy and Security Plan. The Plan was written so that policies and procedures could be set forth Statewide to insure that criminal history record information maintained by any criminal justice agency is complete and accurate and that only authorized agencies or individuals could have access to that data. The Plan also meets Federal rules and regulations which have been set forth governing the collection and dissemination of criminal history information.

The Plan sets forth in detail the policies on dissemination. Criminal history information will only be disseminated to:

- Criminal justice agencies (for certain specified users).
- Other individuals and agencies which require criminal history record information to implement a statute or executive order referring to criminal conduct.
- State or Federal government agencies authorized by statute or executive order to conduct security clearance investigations to determine employment suitability or security clearance eligibility.

Use of criminal history record information disseminated to non-criminal justice agencies will be limited to the purposes for which it was given and shall not be disseminated further.

Upon violation of any rule, policy, or procedure set forth in the Plan by authorized individuals or agencies, the disseminating agency will immediately suspend furnishing any and all criminal history record information. The violating agency or individual will also be subject to a misdemeanor and/or a fine.

User agreements specifically identifying privacy and security terms and conditions will be exercised between every criminal justice agency in the State and the Utah Bureau of Identification (UBI). Criminal justice agencies disseminating criminal history record information to non-criminal justice agencies will exercise a secondary user agreement (as needed).

The Plan identifies procedures to provide for an individual's right to access and review his or her criminal history record information to verify the record's accuracy and completeness.

A certification process is provided within the Plan stating the extent to which Plan procedures have been implemented and detailing the steps undertaken to achieve full compliance.

do not contain a specific reference to a notification requirement, LEAA has interpreted Section 20:21 (c) (2) of the Regulations to require notification to agencies not directly covered by the Regulations. Each disseminating agency subject to the Regulations must give notice of the requirements of the Regulations.

Present Procedures: No procedures are operational.

Proposed Procedures: Criminal history record information will not be disseminated to agencies not directly subject to the regulations unless authorized by State statute or executive order. In those instances, a contractual agreement will be made between the disseminating and receiving agencies stipulating privacy requirements of the Regulations and that sanctions will be imposed. (See Appendix D for samples of the user agreements.) All criminal justice agencies in the State of Utah and applicable non-criminal justice agencies will receive a notice from the Department of Public Safety covering the overall aspects of the Regulations and of the Privacy and Security Plan. The notice will cover topics such as privacy and security, dissemination, right of access and review, user agreements and certification. Subsequent to original notification, when any requirements of the Regulations or the Plan impact the content of the original notice, revised notifications will be sent to all appropriate agencies. An example of how this notice might appear is presented in Exhibit II-1.

C. Audits and Quality Control

The Regulations refer to two types of audits. Section 20:21 (a) (2) refers to systematic audits (e.g. quality controls and audit trails) and Section 20:21(3) requires annual audits of randomly selected criminal justice agencies to determine the degree of compliance with the Regulations.

1. Systematic Audits

LEAA Regulations Requirements: Systematic audits are required by the Regulations to minimize the possibility of recording, storing and disseminating inaccurate criminal history record information. The Regulations also require that all agencies who received inaccurate information be notified. Implied in this requirement is the implementation of a disposition reporting system, delinquent disposition monitoring, audit trails, accuracy checks, document and record inspection and dissemination logs.

Present Procedures: Throughout the State, varying systematic audit procedures are employed by local criminal justice agencies. At the State level, UBI and the State Information Systems Center (the central computer facility) adhere to rigid systematic audit procedures for manual and automated processes.

Manual and automated processes are employed by UBI and the State Information Systems Center to minimize erroneous inputs. Source documents are edited manually to make sure all data fields are complete and correct. Source documents are then coded on coding forms which are randomly edited for accuracy. Coding forms are key-taped for computer input and all key-taped records are verified. All input key-taped records go through normal software editing. Inquiries to the files are logged only by terminal and all transactions entered on-line are logged. All master tapes are stored in the tape library.

Proposed Procedures: Section II A 2 of this Plan describes the procedures to be implemented for disposition reporting and delinquent disposition monitoring. This section of the Plan also describes the procedures to be implemented to provide accuracy checks, document and record inspection and dissemination logs. At the State level, information systems are designed and programmed by the State Information Systems Center. As part of their standard operating procedures, the Center employs a multi-phase design review procedure in which the user agency (in this case a criminal justice agency) is required to review the design, testing and implementation of each information system.

Through the Design Review Procedure of the State Information Systems Center, the criminal justice agency and the Center will review all new criminal history information systems to determine adequacy of systematic audits. This design review will also assure that audit trails are sufficient to trace specific data elements back to the source document. The design review will also certify that audit trails exist to trace all data accesses to the agency and location accessing the information. These provisions are to be reviewed in the systems design phase, tested at system test and reviewed at post-implementation reviews. Prior to December 31, 1976 all existing information systems having access to criminal history data will undergo a similar design review and projects will be scheduled to correct known deficiencies.

Local criminal justice agencies will be encouraged to employ minimum systematic audits in all criminal history record information systems. To aid in this effort, UBI, working with local criminal justice agencies, will develop and distribute systematic audit guidelines.

2. Annual Audits/Compliance Reviews

LEAA Regulations Requirements: Annual audits (compliance reviews) are required by the Regulations to determine the degree of compliance with the Regulations. Also required is the maintenance of appropriate records to facilitate this annual compliance review process.

Present Procedures: No procedures are operational.

Proposed Procedures: The compliance review function for all State and local criminal justice agencies and non-criminal justice agencies (where appropriate) will be performed by a new unit within UBI. Because UBI serves as the Central Repository, another organization will conduct the compliance review of the Central Repository. It has not been determined whether this organization will be a State agency or an independent organization.

These procedures set forth the body of guidelines and standards that are intended for application to audits of all activities and functions which are a part of this Plan -- whether they are performed by individuals employed by State or local governments, independent public accountants or others qualified to perform parts of the compliance review work. These standards relate to the scope and quality of the compliance review.

The individuals selected and assigned to perform the compliance review will collectively possess adequate professional proficiency for the tasks required herein. In all matters relating to the compliance review work, the individuals and their organization will maintain a completely independent and professional attitude. Professional care will be used in preparing the related compliance reports. Consistent with the professional approach, the reviewers will take all precautions necessary to maintain security and confidentiality of criminal history record information.

The following represents the general elements of the audit process to be applied within the compliance review program:

- . The reviewer will select and audit a representative sample of all criminal justice agencies chosen on an unannounced random basis. The audited agencies selected will be considered to be functional (police, courts, corrections, non-profit, etc.) elements of the repository(ies) which are the subject of the specific audit at the time. Both manual and computerized systems within the aforementioned agencies will be audited.
- . Emphasis in this compliance review will be on the application of statistical sampling techniques. In this regard, the auditor will consider the specific number, type, location and size of agencies and/or elements to be audited.
- . The State compliance review staff and the Central Repository reviewer will be responsible for preparing an annual audit plan which will include the provisions of this Plan as a minimum. The audit program will be submitted by the staff for review and approval by the Utah State Commissioner of Public Safety not later than the first day of November for the succeeding calendar year.
- . Written compliance review reports will be submitted to the Utah State Commissioner of Public Safety for review, approval and resolution/clearance.
- . The basic standards and procedures for compliance review (audit) will be as contained in pertinent publications of organizations such as the Comptroller General of the United States, Committee on Auditing Procedures of the AICPA, LEAA and the State of Utah.

The reviewer will inspect and determine the adequacy of internal quality controls (systematic audits) and will determine if the agency:

- . Develops implementing policies, procedures and techniques governing internal control practices to insure security and confidentiality.
- . Establishes adequate controls, uniform definitions, required data and standard procedures to prevent waste and confusion in the collection and presentation of data, as well as assure accuracy and reliability of data.
- . Determines the validity of reported data with basic source data.
- . Employs procedures to assure that all employees who are to handle data are appropriately instructed concerning the sensitive nature of their duties and the data they handle.

On a sampling basis and by actual test of documents, the reviewer will evaluate detailed records such as:

- . Application of dissemination limitations.
- . Application of the individual's rights of access rules.
- . Adequacy of source documentation and records.
- . Adequacy of dissemination logs.

Requirements for data to support the compliance review functions will be identified as part of the annual compliance review program. These data requirements will be identified for all agencies who are subject to the requirements for annual certification.

D. Security and Confidentiality

Section 20:21(f) of the Regulations requires that procedures be implemented to maintain security (physical protection) and confidentiality (controls over dissemination) of criminal history record information. These procedures include consideration of areas such as hardware, software, management, organization, personnel and physical security.

1. Hardware and Software

LEAA Regulations Requirements: The Regulations require

effective and technologically advanced software and hardware designs where computerized processes are employed. The Regulations (in their original form) also require that hardware utilized for processing criminal history record information be dedicated to criminal justice purposes. However, an amendment to the dedication portion of the Regulations (Section 20:21(f)) is pending. This amendment would eliminate the dedicated hardware requirement.

Present Procedures: The Privacy Act of 1974 imposes numerous requirements upon Federal agencies to prevent the misuse of data about individuals, respect its confidentiality and preserve its integrity. The State of Utah, through passage of SB 233 has also recognized the importance of proper handling of data relating to individuals.

The State presently operates a centralized computer facility which serves all State agencies (the State Information Systems Center). The personnel, hardware, software and other facilities in the Center are not dedicated to criminal justice purposes, although the State's criminal history record information system serving the Central Repository operates on the Center's computer.

All criminal history input data to the Central Repository is key entered on key-to-tape devices and audited by UBI. In this case all equipment and personnel are dedicated to criminal justice purposes.

All terminals on-line to the Central Repository's criminal history record information system (which operates on the State Information Systems Center's computer) and all personnel having access to the terminals are dedicated to criminal justice purposes. In some cases, however, the communication lines are shared with non-criminal justice agencies; and in some cases the communication lines are dedicated to criminal justice purposes.

Presently, the Center and the Central Repository employ comprehensive security and confidentiality procedures for all personal and computerized accesses to the Center and its systems. Technologically advanced software and hardware designs are employed for all computerized processes.

Proposed Procedures: The State of Utah believes that actions taken to provide security should be determined

through a risk-assessment process. The intent should be to reduce the security risk as much as possible within the cost and operating constraints of each system dealing with confidential criminal history information. Security provisions should be provided so a criminal justice agency can assure that the security risks associated with its information systems are at an acceptable level.

Security planning relating to criminal history records falls under the broad context of general security planning for all personally identified data handled by the State of Utah. In this respect the guidelines offered in "Computer Security Guidelines for Implementing the Privacy Act of 1974" (FIPSPUB) are considered relevant and applicable in planning for a secure environment for the particular case of criminal justice information systems. This publication is included as Appendix G to this Plan. It is the State's intent to indicate that the guidelines given therein are part of the Utah Plan to provide a secure environment for all criminal history record systems. In the paragraphs to follow, specific implementation of these guidelines are described as they apply to the Regulations.

The following software and hardware procedures will be employed to provide for the security and confidentiality of criminal history records throughout the State of Utah at both the State and local levels:

a. General Security Provisions

Each data center at the State and local levels which processes criminal history information will conduct an annual risk assessment of its general facilities, hardware, system software and management practices. This assessment will be conducted by a representative of criminal justice and data center personnel who are knowledgeable in security procedures. At the State level, personnel designated by the State Systems Planning Steering Board will also participate. This risk assessment, along with managerial response to each risk item and a plan for reducing major risks, will be filed annually with the State Systems Planning Steering Board and the Office of the State Attorney General.

The first general security risk assessment at the State level will be completed prior to April 1976 and annually thereafter. Features of the State Information Systems Center's present operation which pose security risks will be addressed as resources are available. Consideration of security features for hardware and systems software will be included in competitive bid procedures for new computer resources to be conducted during the 1976 calendar year. Provisions for criminal sanctions for security offenses will occur when and if the Legislature feels it is appropriate. However, recommended legislation will be prepared prior to the January 1977 Legislative session. Risk assessments will be conducted at the local level as this Plan is implemented.

The State Information Systems Center provides data processing services for all State agencies and in particular provides services to UBI (who in turn is responsible for the State Central Repository). As a standard practice, the Center employs a multi-phase system development procedure. At each phase of development the user agency is required to review and approve each phase prior to authorizing work on the next phase of the project. It is felt that by the following inclusions to the scope of work presently defined in these Center procedures, security of future criminal history systems can be assured to the degree required. The following procedures are to be added:

- . In the Planning Phase a statement will be provided by the responsible criminal justice agency of the potential results of security violations of the system. The degree of security required and the operating budget available to support special security features will be identified, as well as an ordered list of potential security risks.
- . In the System Design Phase, a statement will be included relating system design features to the security risk statements. A test plan will be outlined to test that the security features function as designed.

- . In the System Test Phase, a special provision will be included that the security tests for system security must be witnessed and signed off by criminal justice personnel in addition to the general sign-off on system functional tests.
- . The post-implementation review will include a review of system security features and a review of the risk-assessments. This review will be filed with the criminal justice agency responsible for the system.

Provisions for review and test of security provisions for State criminal history systems under design will be established prior to January 1, 1977. Guidelines for local system review and security planning will be developed as this Plan is implemented.

It is the intent of the State of Utah to provide a secure environment for the operations of all criminal justice information systems in advance of the December 31, 1977 implementation deadline stipulated in the Regulations.

b. Procedures for Access

The State Information Systems Center and the State Central Repository will continue to utilize comprehensive security and confidentiality procedures for all personal and computerized accesses to their facilities and criminal history records. Because adequate procedures exist at the State level, no major additions are required to adequately control unauthorized access.

During the implementation of this Plan, access guidelines will be developed and distributed to local criminal justice agencies. UBI will promulgate these access control procedures on a State-wide basis as part of their responsibility for Plan implementation.

c. Dedication

The State of Utah's State Information Systems Center employs advanced system software. Present

criminal justice systems have a fair degree of isolation from other systems by allowing access to data files only from authorized terminals or by authorized individuals from the user organization. It is anticipated that advances in systems software in the near future will greatly enhance the ability to offer a virtual resource dedication to a particular user and provide the degree of security that was envisioned by dedicated hardware. However, in the event that these procedures are inadequate (as determined through a system risk-assessment) to provide the necessary degree of security for this and other systems with equally confidential information, it may be necessary for the State of Utah to provide multiple isolated facilities for data files of a confidential nature.

The use of dedicated hardware in order to provide a desired level of security for criminal history records is assumed to be included as an alternative to be considered to reduce the risk of unauthorized access to file information from unauthorized users. In making the determination of adequacy of hardware/software facilities, it would be helpful to have a definition of acceptable levels of risk identified by LEAA and an identification of how much resources would be made available in the event that costly system additions were required.

The State of Utah does not intend to follow a policy of dedicated hardware for the sole purpose of meeting a requirement for dedicated hardware which is not based upon specific cost/benefit related criteria. Also, UBI will not promulgate dedicated hardware to local criminal justice agencies as the only method which could be used to provide adequate security and confidentiality controls of criminal history record information systems. The State will continue to build upon its present use of technologically advanced system software and access management procedures to provide required controls; and UBI will develop relevant guidelines and will promulgate their use by local criminal justice agencies.

2. Management Control and Designation of the Responsible Agency

LEAA Regulations Requirements: The Regulations require that a designated criminal justice agency have overall responsibility for the privacy and security of criminal history record information. This agency would also be required to exercise certain other controls over the hardware, software and personnel involved with criminal history records. Such an agency would be designated wherever criminal history record information is collected, stored or disseminated. However, an amendment to this requirement is anticipated.

Present Procedures: Under present procedures at the State level, the Department of Public Safety has the power to veto, for legitimate purposes, which personnel can be permitted to work in any area where sensitive criminal justice information is stored; including the State Information Systems Center. They do not have, however, the power to veto personnel in the various city or county computer centers, which may be part of the criminal justice information system network.

At the level of the Central Repository, UBI has the authority to assure that an individual or agency authorized direct access is administratively held 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 accesses, disclosure or dissemination. The same control is much more difficult for information not stored in the Central Repository. The authority to set and enforce policy concerning computer operations at the level of State agencies is vested in the State Systems Planning Steering Board. The authority to affect the Plan's policies would have to be obtained from that agency under present Utah law.

Proposed Procedures: It is felt that the present provisions of Utah law are sufficient to provide a secure environment at the State level. However, additional understandings will have to be obtained in order to assure that county and city operations are functioning in a secure environment. This may be obtainable through contract agreements with the various centers involved, which would allow for certain auditing or personnel background checks to be employed where those centers handle criminal justice information.

3. Personnel

LEAA Regulations Requirements: The Regulations require

that a criminal justice agency will select and supervise all personnel authorized to have direct access to criminal history record information.

Present Procedures: At the State and local levels, each criminal justice agency selects, supervises and trains all personnel having direct access to criminal history record information. In addition, it is the prerogative of the Utah Department of Public Safety to conduct a background check on personnel of the State Information Systems Center who may constitute a security risk. Persons challenged as a result of such checks are terminated or are reassigned to low risk areas. Access to criminal justice information systems via terminals on-line to the Center's computer is limited to authorized personnel who are under the control of a criminal justice agency at the State and local levels.

Proposed Procedures: Present personnel procedures in State and local criminal justice agencies are adequate to ensure proper confidentiality of criminal history record information. However, where computers are employed at the local level by a centralized computer center, procedures similar to those employed at the State level should be implemented. During the Plan's implementation, UBI will promulgate the use of such a policy.

4. Physical Security

LEAA Regulations Requirements: The Regulations require procedures to protect against unauthorized access, theft, sabotage, fire, flood, wind or other natural or man-made disasters.

Present Procedures: At the State level, the State Information Systems Center (the central computer facility) has a comprehensive and highly secure set of physical security features. All operations staff who are authorized access to the computer room may enter through one of two doors which are activated by an electronic pass card device. All visitors, including personnel such as the Center's Director, programming personnel and outside visitors, must log in and out and must be accompanied by an authorized representative from the Center. The Center is protected against unauthorized access, theft, fire, flood and wind. The Center is fully enclosed with no windows. All of the Center's interior is protected from fire by an advanced Haylon fire detection and fire suppressant system. Also, there is an emergency lighting system.

Although tapes and other data files are not kept in a fireproof vault, they are protected from fire by the Haylon system and are not vulnerable to theft from outside personnel. Also, all major files have back-up copies stored several miles away in a highly secure and fireproof vault. The Center is presently seeking budgetary support to add an emergency auxiliary power system and to hire a full-time, on-site security guard.

The State does not have jurisdiction over computer facilities at the local level and cannot attest to the degree of effectiveness of the physical security features of these local facilities. However, the majority of the local computer facilities do employ comparable security measures which run the full spectrum of highly secure to less than secure.

Proposed Procedures: As discussed in Section II D 1 of this Plan, the State intends to develop and maintain its security measures based upon the risk-assessment philosophy as described. Also, the State intends to follow the physical security guidelines contained in "Computer Security Guidelines for Implementing the Privacy Act of 1974" (see Appendix D). Presently, the State Information Systems Center employs fully adequate physical security measures and no major improvements are deemed necessary. During the course of implementing this Plan, the physical security features of local computer facilities will be appraised during the risk-assessment process for the local criminal justice agencies. Also, UBI will promulgate the use by local criminal justice agencies and local computer facilities of the security and confidentiality policy guidelines developed for use by these local agencies.

E. Individual Right of Access and Review ____

Section 20:21(g) of the Regulations provides for an individual's right to access and review their criminal history record to verify the record's accuracy and completeness. The Regulations stipulate certain conditions regarding verification of identity, rules for access, point of review, review mechanism, challenge, administrative review and record correction, appeal procedures and information subject to review. Section 20:22(b)(1) of the Regulations requires the access and review procedures to be completely operational upon the due date for Plan submission (March 16, 1976).

UBI will implement all of the access and review procedures outlined in Section II E of this Plan. These procedures will be effective as of March 16, 1975.

1. Verification of Identity

LEAA Regulations Requirements: The Regulations do stipulate that, "upon satisfactory verification of his identity...", any individual shall be entitled to review any criminal history record information maintained about the individual. LEAA has interpreted the "satisfactory verification" provision to mean that fingerprint comparison is not mandatory and that each state is free to use any appropriate verification method.

Present Procedures: There are no uniform procedures currently operational. However, individuals are allowed to review criminal history records by criminal justice agencies throughout the State. Each agency employs its own procedures for verification of identity.

Proposed Procedures: Individuals desiring to access and review their criminal history record must present themselves to a law enforcement agency or to UBI. An individual must fill out an application form prescribed by UBI. This application form is currently under development by UBI and it is anticipated that a three-part form will be used. If the applicant is unable to write, someone else may complete the application form; however, the applicant must be present at the time of application to attest to the application's accuracy.

Before an individual views their criminal record at a law enforcement agency, their identity must be verified by an employee of that agency who personally knows the individual; otherwise, it must be verified by a fingerprint match or by another method approved in advance by the Director of UBI. If an individual comes to UBI to view his criminal record, verification of his identity by fingerprint match will be the only acceptable method. In cases where an individual is physically incapable of giving fingerprints, verification of identity may be by other methods approved by the Director of UBI. All fingerprint matches must be made by a technician certified by UBI as one qualified in fingerprint comparison. If the agency has no qualified technician, the application, bearing plain impressions of one hand, must be forwarded to UBI for comparison and certification of identity.

UBI will make the fingerprint comparison and certify when the fingerprints match. If the certification states the fingerprints match, the applicant may then see the record; otherwise, the applicant will not be authorized to see the record. UBI will return the application to the law enforcement agency.

2. Rules for Access

LEAA Regulations Requirements: Rules for access are not identified in the Regulations, although LEAA has interpreted the Regulations to require the development of written rules which set forth the procedures for access and review. These rules must be made publicly available such as by publication or by distribution of pamphlets.

Present Procedures: No uniform procedures are operational. However, criminal justice agencies throughout the State apply their own rules for allowing access to criminal history record information.

Proposed Procedures: The procedures for an individual to access and review their criminal history record will be printed by UBI and distributed to all criminal justice agencies and other selected non-criminal justice agencies within the State. The distribution will also include a supply of forms to be filled out by the applicant. UBI will print posters announcing the individual's right of access and review and outlining the procedures to be followed. The posters will be distributed to all criminal justice agencies and selected non-criminal justice agencies with a request that they be posted in locations most convenient for the public to see them. Formal public notification of an individual's right of access and review and the procedures to follow will be accomplished through Utah's Administrative Rule Making process in accordance with Utah Code Annotated 1953 as amended, Title 63, Chapter 46 - Administrative Rule Making. This process requires that certain specific steps be taken to implement new rules. These include steps such as filing an official record of the rule, making the rule available for public inspection and allowing public opinions about the rule prior to adoption of the rule. Upon official adoption of the rules for access, a news release will be prepared and included with a request that it be publicized on March 16, 1976.

3. Point of Review and Mechanism

LEAA Regulations Requirements: The Regulations provide for review "without undue burden to either the criminal justice agency or the individual." LEAA has interpreted this to mean that the individual bears the burden of justifying his need for a copy of his criminal history record for challenge purposes. If a copy is provided, a fee may be charged which covers actual copy making costs.

Present Procedures: No uniform procedures are operational. However, individuals presently are allowed to review criminal history records at most criminal justice agencies throughout the State where criminal history records are maintained.

Proposed Procedures: An individual may appear in person at any law enforcement agency or UBI and apply to access and review his criminal history record at any time during normal day time working hours or as specified by that agency. The individual must fill out the application form prescribed by UBI and pay the prescribed fee. The applicant will be provided a receipt. If the record access and review can be accomplished at that agency the fee shall be an amount set by it. The money shall be accounted for by a method according to local accounting policy. If the access and review is accomplished at UBI the fee is \$10.00 which must be promptly deposited in the State Treasury and credited to the General Fund.

If the law enforcement agency does not have the individual's complete record to review, the application and a \$10.00 fee will be forwarded to UBI where identity will be verified by fingerprint match. At the discretion of each law enforcement agency, they may charge an additional service fee.

Upon receiving an application, UBI will review the subject's record to determine if it is accurate and complete. If it appears that all dispositions are not reported, UBI will follow-up as necessary to obtain the required dispositions which will be recorded on the individual's criminal history record. When a complete and accurate record is available, a copy of the record and the application form will be returned to the requesting agency. If the prints on the application form do not match with those in the requested record, only the application form will be returned to the requesting agency.

Upon request, the individual will be provided a copy of

his criminal history record. If the copy is for challenge purposes the law enforcement agency will follow the challenge procedure described in Section II E 4 of this Plan.

If the law enforcement agency has the ability to provide a copy of an individual's record at the time of application, and a copy is required, an immediate copy will be provided. Otherwise, the individual will have to wait for UBI to send a copy to the law enforcement agency.

4. Challenge

LEAA Regulations Requirements: The Regulations identify an individual's right to challenge the accuracy and completeness of the individual's criminal history record.

Present Procedures: No uniform procedures are operational.

Proposed Procedures: If an individual challenges the accuracy or completeness of their record, the person must so indicate on that portion of the application form provided for challenge. The individual must state the nature of the disagreement and give a correct version of their record and explain why they believe their version to be correct. It is assumed that the individual will have already obtained a copy of their criminal history record for this purpose, and that the copy of the record has been stamped to indicate it is for review and challenge only. This notification will also indicate that any other dissemination or use is in violation of State rules and regulations and/or State and Federal law. A copy of the challenged application form will be sent to UBI, a copy will be given to the individual, and the law enforcement agency will retain the original copy.

Upon receipt of the challenge, the criminal justice agency will review the individual's statement. If it is determined that the criminal history record should be corrected, appropriate steps will be taken by the criminal justice agency to cause the official record to be corrected. After correction, the individual will be required to review the corrected record without additional cost to the individual and attest in written form that the record is now correct and to retract the challenge status. Also, a corrected copy will be sent to any other agencies who have received an incorrect copy of the individual's record.

If the criminal justice agency disagrees with the individual's challenge and will not correct the record, the individual must then follow the administrative review procedure described in Section II E 5 of this Plan to effect a correction of their record.

5. Administrative Review and Record Corrections

LEAA Regulations Requirements: The Regulations require the establishment of procedures for administrative review and correction of inaccurate information claimed by an individual.

Present Procedures: No uniform procedures are operational.

Proposed Procedures: An Administrative Review Board will be appointed by the State's appointing power. The membership of the Board and the tenure of the Board will be determined by the State's appointing power.

In the event a criminal justice agency refuses to correct the challenged information, the individual will have the right to an administrative review by making a written request. The review shall take place within 30 days of the Board's receipt of the administrative review request.

The Board will complete an audit of the individual's record sufficient to determine the accuracy of the challenge and will forward a written report to the contributing agency and the individual. Should the audit disclose inaccuracies or omissions in the official record, the criminal justice agency will be required to cause appropriate alterations or additions to be made. The Board will provide written notice of its actions to UBI and the individual and UBI will be required to correct the Central Repository record. Any other agencies to which the criminal history record has previously been disseminated will be forwarded a corrected copy by UBI.

If the written report of the audit indicates no errors or omissions and the individual still holds to his challenge, they may appeal in writing, following the procedure described in Section II E 6 of this Plan.

6. Appeal

LEAA Regulations Requirements: In cases of conflict between an individual and a criminal justice agency who refuses to correct the individual's challenged criminal history record, the Regulations require formal appeal procedures.

Present Procedures: No uniform procedures are operational.

Proposed Procedures: If the Administrative Review Board upholds the position of a criminal justice agency and agrees that an individual's criminal history record is correct, and the individual still believes their record to be incorrect, the individual has one final administrative step he may follow. The individual may appeal the Board's decision in writing to the Commissioner of Public Safety. The appeal will be conducted in accordance with the State Uniform Hearing Procedures rules as written by the Utah Attorney General in accordance with Section 63-46-11, Utah Code Annotated 1953. The appeal will be conducted within 30 days of the Commissioner of Public Safety's receipt of the written request for appeal and the findings of the Commissioner will be final. Prior to March 16, 1976 the Commissioner of Public Safety will request instructions from the Utah Attorney General which describe the mechanics of the actual steps in the appeal process.

If the results of the appeal are in favor of the individual, the Commissioner of Public Safety will require that the criminal justice agency cause appropriate alterations or additions to be made. The Commissioner will provide written notice of his actions to UBI and the individual and UBI will be required to correct the Central Repository record. Any other agencies to which the criminal history record has previously been disseminated will be forwarded a corrected copy by UBI. If the appeal upholds the decision of the Administrative Review Board, the Commissioner will notify the criminal justice agency, the individual and UBI of his findings. If the individual still wishes to arbitrate this final decision, the individual will have to pursue legal action through the courts.

7. Correction

LEAA Regulations Requirements: The Regulations require

that all criminal justice agencies receiving an incorrect criminal history record be notified when incorrect criminal history record information is discovered; this requirement does not pertain to non-criminal justice agencies who received the incorrect information. However, Section 20:21(g)(4) provides that an individual may request a list of all non-criminal justice agencies who received the incorrect information.

Present Procedures: No formal procedures are operational. However, UBI and criminal justice agencies presently cooperate to the maximum extent possible in the correction of inaccurate criminal history records.

Proposed Procedures: Upon receipt of an official written communication directly from the criminal justice agency which contributed the original information or upon direction from the Administrative Review Board or from the Commissioner of Public Safety, UBI will make any correction or additions necessary to comply with the official record. When a criminal justice agency (other than UBI) receives official written communication directly from the Administrative Review Board or from the Commissioner of Public Safety, the criminal justice agency will make any required correction or additions to the record. This process will also be followed upon court order.

A copy of the corrected record will be sent to all agencies who have previously been furnished a copy. Upon request, the individual whose record has been corrected will be given the name of all non-criminal justice agencies who received a copy of the incorrect record.

If any criminal justice agency discovers that they have submitted incorrect criminal history data to UBI, they will immediately forward the correct information to UBI. UBI will correct its records and furnish the correct record to any agency previously receiving an incorrect copy of the record.

As UBI carries out its responsibility as the Central Repository and discovers that an error has been made, the record will be corrected. A corrected copy of the record will be furnished to any agency previously receiving an incorrect copy of the record.

8. Information Subject to Review

LEAA Regulations Requirements: The Regulations limit the information an individual may review about the individual's criminal history. An individual may not have access to criminal history record information contained in "intelligence, investigatory or other related files and shall not be construed to include any other information than that defined by (Section) 20.3(b)." This means that an individual may review information related only to the fact, date and results of each stage of the criminal justice process through which the individual passed.

Present Procedures: Present statutes do not provide for any information to be subject to review.

Proposed Procedures: An individual's right of review extends only to criminal history record information concerning them. Therefore, an individual will be limited to a review of the fact, date and results of each formal stage of the criminal justice process through which they passed to ensure that such steps are completely and accurately recorded. Legislative or executive action is required to implement this procedure.

F. Certification Statement

Section 20:22 of the Regulations requires that the State provide a certification with the Plan's submission that action has been taken to comply with the Plan's procedures to the maximum extent feasible. Section 20:23 requires certifications to be submitted to LEAA in December of each year to update the prior year's submission. Although the Regulations require all features of the Plan to be fully operational by December 31, 1977, a state may make written application for an additional period of time to fully operationalize the state plan. In the case where such an extension were granted, the annual certifications are still required. The Regulations identify the specific components which must be included in the certification. At a minimum, the certification must state that the procedure for access and review under Section 20:21(g) of the Regulations are fully operational.

1. Applicable Criminal Justice and Non-Criminal Justice Agencies

LEAA Regulations Requirements: The Regulations do not specifically require the identification of these agencies; however, such identification is implicit in the requirement to conduct the certification process.

**EXHIBIT II-2 : SUMMARY OF CERTIFICATION
APPLICABILITY CRITERIA DETERMINATION SURVEY**

Agency Groups	Total Number of Agencies In Each Applicability Criteria Category													Totals and Percentages		
	1	2	3	4	5	6	7	8	9	10	11	12	13	Total Sent	Total Rec'd	% Rec'd
Sheriffs Offices		4	2	1	2	17							3	29	29	100.0
Police Depts.	21	4	3	3	7	40	1						6	154	85	55.2
Justices of the Peace	40	7	1	8	1	6	1							180	64	35.6
City Courts	3	1	3		1	2								15	10	66.7
County Clerks	9	2	2		4	5								29	22	75.9
City and County Attorneys	15	3		7	4	4							1	58	34	58.6
State Agencies	1			1	1	1	1						3	8	8	100.0
Grand Total	89	21	11	20	20	75	3						13	473	252	53.3
Summary Total	121			118					13					473	252	53.3

SUMMARY ANALYSES

TYPE OF ANALYSES	Total Number of Agencies By Applicability Criteria Grouping			Totals and Percentages		
	1 - 3 Totally Unaffected by LEAA Regulations	4 - 8 Only Require User Agreements	9 - 13 Require Certification	Total Sent	Total Rec'd	% Rec'd
Total Number of Agencies	121	118	13	473	252	53.3
Received as a % of Total Sent	25.6%	24.9%	2.8%	473	252	53.3
Received as a % of Total Received	48.0%	46.8%	5.2%		252	100.0

Present Procedures: Comprehensive certification procedures are operational. These procedures were developed concurrently with the Plan's development to meet the Regulations' certification requirement. The following are summarized statements of the procedures used to conduct the certifications:

- . A list of all applicable agencies was developed (see Appendix H).
- . A procedure was developed to determine the extent the Regulations affect an agency and the degree of certification necessary (see Appendix I).
- . A certification applicability criteria determination survey form and letters of explanation were developed for mailing to all agencies identified in Appendix H (see Appendix J). All respondents to the survey, also noted in Appendix H, were then applied to the Appendix I procedure to determine which agencies were unaffected by the Regulations, required user agreements or required some form of certification; a checklist was used for this purpose to evaluate all survey respondents (see Appendix H).
- . A determination was made of the extent an agency had to comply with each element of the Plan on the basis of the agency's response to the survey. It is possible for an agency to require one of five certifications as presented in Appendix K. The "X" or "C" in a column opposite the Plan's procedures definition indicates under each certification process the extent of compliance required.
- . The results of the survey were summarized to allow for overall appraisal of the requirements for certification. Based upon this analysis, and a trial certification, the total certification work effort was determined. These results are presented in Exhibit II-2.
- . The actual certification procedure involved on-site visitations to all agencies requiring certification. During these on-site visits the person conducting the certification determined the accuracy of the agency's responses

to the original survey to be positive of the certification process required. Once the precise certification process requirement was determined, the certification was completed following the procedure presented in Appendix L.

The Agency List/Certification Process Requirement checklist contains a comprehensive list of each criminal justice agency in the State with an indication of each agency who responded to the applicability determination criteria survey (see Appendix H). A determination was made that the agencies identified in Appendix H as requiring certification were, in fact, the only agencies requiring certification.

One hundred percent response to the survey was received from only State agencies and County Sheriff offices. Of the Police Departments who did not respond to the survey, it was determined that none of those remaining would require certification because they are all one-man type departments who would not fall into a certification category. Of the Justices of the Peace who did not respond to the survey, it was determined that none of these remaining would require certification because those who responded were a representative sample and none who responded required certification. Of the court agencies who did not respond to the survey, it was determined that none of those remaining would require certification because those who responded were a representative sample and none who responded required certification. Of the city and county attorneys who did not respond to the survey, it was determined that none of those remaining would require certification because those who responded were a representative sample and none who responded required certification (with the exception of the Salt Lake County Attorney who is a terminal site).

There are thirteen agencies throughout the State with on-line terminal capability. All of these agencies' responses to the survey placed them in a certification-required status.

The same basic procedure will be used to conduct the annual certifications. However, refinements in the procedure will be developed as appropriate.

Proposed Procedures: The procedures developed as described above will continue to be used. Further development of these procedures is not required.

2. Certification Checklist for the State Central Repository

LEAA Regulations Requirements: The Regulations do not contain a specific reference to a checklist. However, the Regulations do require "an outline of the action which has been instituted." LEAA has interpreted this requirement's intent can be fulfilled through the use of a checklist as a feature of the certification process.

Present Procedures: Following the Master Certification Elements identified in Appendix K, the Central Repository was certified following the certification procedure for the Central Repository as defined on the form/process identified in Appendix L.

The actual certification procedure used was as follows:

- . A small Certification Team of State personnel from the Department of Public Safety were trained in the methods of the certification form/process identified in Appendix L.
- . The Certification Team were provided copies of this Criminal History Privacy and Security Plan and familiarized themselves with the elements of the procedures outlined in the Plan.
- . The Certification Team then made an on-site visitation to the Central Repository (UBI) and completed the Central Repository certification form/process form. A copy of this completed form is contained in Appendix N.
- . The signature of the head of the Central Repository was obtained to formalize the certification and to signify the extent that the procedures in the Plan have been implemented in the State.

The same basic procedure will be used to conduct the annual certifications. However, refinements in the certification procedure and the certification form/process form will be developed as appropriate.

Proposed Procedures: The procedures developed as described above will continue to be used. Further development of these procedures is not required.

3. Certification Checklists for Other Agencies

LEAA Regulations Requirements: The Regulations do not contain a specific reference to a checklist. However, the Regulations do require "an outline of the action which has been instituted." LEAA has interpreted this requirement's intent can be fulfilled through the use of a checklist as a feature of the certification process.

Present Procedures: Following the Master Certification Elements identified in Appendix K, each criminal justice agency listed in Appendix J who fell within the nine through thirteen certification applicability criteria range was certified following the certification procedures as defined on the form/process identified in Appendix L.

The actual certification procedure used was as follows:

- . A small Certification Team of State personnel from the Department of Public Safety were trained in the methods of the certification form/process identified in Appendix L.
- . The Certification Team were provided copies of this Criminal History Privacy and Security Plan and familiarized themselves with the elements of the procedures outlined in the Plan.
- . Each member of the Certification Team was assigned a group of criminal justice agencies to certify and a visitation date was scheduled in advance with each agency.
- . Prior to visiting each criminal justice agency, these agencies were contacted to verify the accuracy of the agencies' responses to the original certification applicability criteria determination survey; also, these responses were again verified during the Certification Team's on-site visits.
- . The certification procedures were tested in a selected criminal justice agency to refine the forms and procedures prior to final procedure implementation.

- . The Certification Team then made on-site visitations to each criminal justice agency requiring certification and completed the certification form/process form. A copy of each of these completed forms is contained in Appendix N.
- . The head of each criminal justice agency signed and dated the certification form/process form for their agency to attest to the accuracy of the certification.

The same basic procedure will be used to conduct the annual certifications. However, refinements in the certification procedure and the certification form/process form will be developed as appropriate.

Proposed Procedures: The procedures developed as described above will continue to be used. Further development of these procedures is not required.

4. Legislation Dealing with Plan Compliance

LEAA Regulations Requirements: The Regulations require a description of any legislation, executive order or other action taken to obtain authority to comply with the Regulations.

Present Procedures: No legislation is pending relative to Plan implementation. The next Legislative session for this purpose will not begin until January 1977.

Proposed Procedures: Many of the procedures and policies in this Plan can be implemented within the framework of existing laws and authorities. However, some features in the Plan will require legislation and/or Executive orders to implement the Plan. During the initial months of the Plan's implementation, these legislative and Executive requirements will be defined in detail prior to the 1977 Legislative session. Where possible, Executive actions will be taken prior to January 1977.

5. Other Legislation/Executive Orders for Non-Criminal Justice Users for Dissemination of Criminal History Data

LEAA Regulations Requirements: The Regulations require an identification of all non-criminal justice dissemina-

tion authorized by existing legislation. This identification should include the specific categories of non-criminal justice agencies or individuals, the specific purposes or uses of disseminated information and citations of the statutory or executive orders.

Present Procedures: A review was conducted of existing State statutes to determine if any authority exists which provides for or prohibits dissemination of criminal history record information to non-criminal justice agencies. It was determined that no statutory reference is made to dissemination of criminal history record information to non-criminal justice agencies.

Proposed Procedures: No additional work is required to document this area of existing authority dealing with non-criminal justice dissemination.

6. Progress Toward Problem Resolution

LEAA Regulations Requirements: The Regulations require a description of the action which has been taken by the State to achieve the development of complete and accurate criminal history record information. These actions would include the steps taken to overcome any fiscal, technological or administrative barriers. A major portion of this description will relate to the action the State has taken to implement a disposition reporting system.

Present Procedures: Legislative actions can be taken in January 1976 to solve the fiscal problems for UBI to start Plan implementation. The Department of Public Safety is seeking an augmentation to their 1975-76 budget to provide some initial staffing within UBI to begin Plan implementation. Also, the Department has included additional new positions in their 1976-77 budget which is pending approval by the Legislature in January 1976.

The State is in the process of implementing a disposition reporting system which is planned for Statewide implementation by October 1976. A disposition reporting form is being developed (see the Utah Arrest and Court Disposition Report contained in Appendix C) that will follow a defendant through the judicial

process and report disposition information to the Central Repository as the defendant passes through the criminal justice system. This system will be fully responsive to the requirements in the Regulations. Also, the right of access procedures will be operational by March 16, 1976.

No other actions have been taken by the State or by local criminal justice agencies toward problem resolution. However, as soon as the additional UBI staff are hired (assuming the budget request is approved by the Legislature) the Plan's implementation will be aggressively pursued.

G. Relevant Statewide Criminal Justice System Standards and Goals

The Regulations do not specifically require procedures regarding these privacy and security standards and goals. However, the Utah Council on Criminal Justice Administration has formally adopted specific Criminal Justice System standards. Certain of these standards are relevant to the requirements and recommended procedures contained within the Regulations.

Within the Privacy and Security standards, minimum acceptable levels of system security and privacy protection are established. These standards provide for legislation to: support the security and privacy consideration of criminal justice information systems; limit access and dissemination of information; provide for the right of information review and corresponding procedures; classify data; provide security precautions; and define what information is available for research from the system. The issues of quality of data, completeness and accuracy of data, and separation and isolation of the complete criminal justice file are addressed in the standards on operations. Technical system design standards establish: appropriate communication levels among criminal justice agencies in relation to standard data elements; specific program language requirements; and resources to assure adequate teleprocessing capabilities. Implementation strategy standards address the issues of establishing statutory authority and administrative action in the planning, development, coordination, and operation of State level information systems.

Listed in Appendix M are the relevant Utah standards, a narrative on current status and comments of each, and the implementation methodology. Implementation of these selected standards will assist the Statewide effort directed toward achieving full compliance with the Regulations.

III. SCHEDULE OF MAJOR MILESTONES

This section describes the timetable and major milestone events in bringing all agencies into compliance with the Regulations. The approach used is a schedule of major action steps to be taken displayed over time which result in major milestone events. This Action Plan and Schedule is presented in Exhibit III-1.

The certification forms for each criminal justice agency who require certification provide for an estimated date for each of the relevant procedures in the Privacy and Security Plan to be fully operational in each agency (see Appendices N and O). This date is indicated whenever a criminal justice agency could make a specific commitment to operationalize the Plan's procedure; where a date is not indicated the agency was unable, at this time, to make a specific implementation commitment because of the constraints now present. A December 31, 1977 date could have been used in these constraint situations, but it will be more valuable to the Plan's implementation to know exactly where Plan implementation problems exist.

The major tasks required to implement the Privacy and Security Plan on a Statewide basis are listed in Exhibit III-1. The milestones resulting from these tasks, which are related to Privacy and Security Plan implementation, are also identified in Exhibit III-1. It is important to point out that the Exhibit III-1 Action

Plan incorporates the work activities necessary to implement the Privacy and Security Plan throughout the State; not limiting implementation to just those criminal justice agencies who are subject to the Regulations.

The Action Plan provides for an identification of the time period (month or year) for conducting each of the major tasks and the target date for each milestone. This schedule information is indicated on the Action Plan wherever it was possible to identify when these events could actually be executed; where this schedule information is not indicated it was not possible, at this time, to make a specific schedule commitment because of existing constraints or other unknowns. When implementation of the Privacy and Security Plan begins, these scheduling unknowns and constraints will be analyzed and the Action Plan will be refined and presented in complete detail.

EXHIBIT III-1: ACTION PLAN AND SCHEDULE

MONTH/YEAR OF ACTION ACTIVITY

ACTION ACTIVITY																									
No.	Description	'76 Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	'76 Dec	'77 Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	'77 Dec	Milestone Events	
1	<u>COMPLETENESS AND ACCURACY</u>																								
1.1	Formally designate UBI as the State Central Repository																							1. <u>March 16, 1976</u> : State Central Repository fully operational	
1.2	Develop detailed procedures for the Disposition Reporting System																							2. <u>July 31, 1976</u> : User agreements executed between all appropriate parties	
1.3	Develop detailed procedures for the Delinquent Disposition Monitor program																							3. <u>October 31, 1976</u> : Disposition Reporting System fully operational	
1.4	Develop disposition reporting and delinquent disposition monitoring guidelines for criminal history record systems in use in criminal justice agencies other than the Central Repository																							4. <u>March 31, 1977</u> : Delinquent Disposition Monitoring procedures fully operational	
1.5	Refine the user agreement form																							5. <u>December 31, 1977</u> : Procedures for maximizing the completeness and accuracy of record dissemination are fully operational	
1.6	Execute user agreements between the Central Repository and every criminal justice agency in the State																								
1.7	Execute user agreements between the Central Repository and authorized non-criminal justice agencies																								
1.8	Advise criminal justice agencies of the requirement for their executing user agreements with authorized																								

EXHIBIT III-1: ACTION PLAN AND SCHEDULE

MONTH/YEAR OF ACTION ACTIVITY

ACTION ACTIVITY																								
No.	Description	'76 Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	'76 Dec	'77 Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	'77 Dec	Milestone Events
	non-criminal justice agencies as required																							<div>1. <u>December 31, 1976</u> : Notices sent to all State and local criminal justice agencies</div> <div>2. <u>December 31, 1977</u> : Procedures which limit dissemination to authorized agencies are fully operational</div>
1.9	Implement the Disposition Reporting System and the Delinquent Disposition Monitor program																							
1.10	Implement other Plan procedures required to maximize the completeness and accuracy of disseminated criminal history record information																							
1.11	Enact legislation and/or issue executive orders as required to fully implement all Plan procedures dealing with Completeness and Accuracy																							
2.	<u>LIMITS ON DISSEMINATION</u>																							
2.1	Develop detailed procedures for criminal justice agencies to limit criminal history record information dissemination																							
2.2	Develop detailed procedures for criminal justice agencies to validate an agency's right of access																							
2.3	Prepare and distribute notices to all criminal justice agencies and to appropriate non-criminal justice agencies																							

EXHIBIT III-1: ACTION PLAN AND SCHEDULE

MONTH/YEAR OF ACTION ACTIVITY

ACTION ACTIVITY																								
No.	Description	'76 Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	'76 Dec	'77 Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	'77 Dec	Milestone Events
2.4	Define specific sanctions and develop any required drafts of legislation and/or executive orders																							
2.5	Enact legislation and/or issue executive orders as required to fully implement all Plan procedures dealing with Limits on Dissemination																							
3.	AUDITS AND QUALITY CONTROL																							
3.1	Select organization who will conduct the annual Regulations compliance review of the State Central Repository																							1. August 31, 1976 : Staff hired and organizational framework implemented for conducting annual Regulations compliance review
3.2	Develop detailed compliance review/audit program and procedures																							2. December 31, 1976 : Systematic audit methodoligies are employed in all existing and new State Criminal History Record Information Systems
3.3	Implement new Design Review Procedures required for incorporation of systematic audits in all State criminal history record information systems																							3. January 2, 1977 : Begin to conduct annual Regulations compliance reviews/ audits
3.4	Develop systematic audit guidelines for distribution to local criminal justice agencies																							4. October 31, 1977 : Develop and implement a program to assist local criminal justice agencies in the application of systematic audit methodolgies for Criminal History Record Information Systems
3.5	Conduct annual Regulations compliance review/audit of State Central Repository																							

1. August 31, 1976 : Staff hired and organizational framework implemented for conducting annual Regulations compliance review
2. December 31, 1976 : Systematic audit methodologies are employed in all existing and new State Criminal History Record Information Systems
3. January 2, 1977 : Begin to conduct annual Regulations compliance reviews/audits
4. October 31, 1977 : Develop and implement a program to assist local criminal justice agencies in the application of systematic audit methodologies for Criminal History Record Information Systems

EXHIBIT III-1: ACTION PLAN AND SCHEDULE

MONTH/YEAR OF ACTION ACTIVITY

ACTION ACTIVITY																									
No.	Description	'76 Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	'76 Dec	'77 Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	'77 Dec	Milestone Events	
3.6	Conduct annual Regulations compliance review/audit of selected local criminal justice agencies																								
3.7	Enact legislation and/or issue executive orders as required to fully implement all Plan procedures dealing with Audits and Quality Control																								
4.	SECURITY AND CONFIDENTIALITY																								
4.1	Define the security and confidentiality risk-assessment methodology to be employed at the State and local levels																								
4.2	Define specific State oriented security and confidentiality policies as derived from the FIPSPUB guidelines (See Appendix G of the Plan)																								
4.3	Develop security and confidentiality policy guidelines for distribution to local criminal justice agencies (as derived from the FIPSPUB guidelines)																								
4.4	Select several local criminal justice agencies who would volunteer to implement the security and confidentiality policies on an experimental basis																								
<div>1. <u>March 31, 1976</u> : Develop a security and confidentiality risk-assessment analysis for Criminal History Record Information Systems at the State and local levels</div> <div>2. _____ : Specific security and confidentiality policies are implemented for the State Central Repository, State Information System Center, and remote criminal justice terminal sites</div> <div>3. _____ : Develop security and confidentiality policy guidelines for local criminal justice agencies and begin Statewide implementation on an experimental basis in selected pilot agencies</div> <div>4. <u>December 31, 1977</u> : To the extent feasible, procedures are fully operational which provide security and confidentiality of Criminal History Record Information</div>																									

EXHIBIT III-1: ACTION PLAN AND SCHEDULE

MONTH/YEAR OF ACTION ACTIVITY

ACTION ACTIVITY																									
No.	Description	'76 Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	'76 Dec	'77 Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	'77 Dec	Milestone Events	
4.5	Evaluate the results of the experimental program																								
4.6	As determined to be appropriate, continue to promulgate the implementation of security and confidentiality policies on a Statewide basis																								
4.7	Conduct the annual risk assessment for the State Central Repository																								
4.8	Assist local criminal justice agencies who have computer facilities with the preparation of annual risk assessments																								
4.9	Enact legislation and/or issue executive orders as required to fully implement all Plan procedures dealing with Security and Confidentiality																								
5.	<u>RIGHT OF ACCESS AND REVIEW</u>																								
5.1	Develop proposed detailed procedures for access and review following the guidelines contained in Section II E of the Plan																								
5.2	Execute the required Rule Making process prior to formal adoption of the access and review procedures																								

1. March 16, 1976 : Procedures are fully operational to allow an individual to exercise their right of access and review of criminal history record information

1. March 16, 1976 : Procedures are fully operational to allow an individual to exercise their right of access and review of criminal history record information

EXHIBIT III-1: ACTION PLAN AND SCHEDULE

MONTH/YEAR OF ACTION ACTIVITY

ACTION ACTIVITY

No.	Description	'76 Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	'76 Dec	'77 Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	'77 Dec	Milestone Events
5.3	Distribute final, approved access and review procedures and forms to all criminal justice agencies and other selected non-criminal justice agencies																							
5.4	Print and distribute announcement posters																							
5.5	Prepare and circulate news release for publication on March 16, 1976																							
5.6	Enact legislation and/or issue executive orders as required to fully implement all right of access and review procedures on March 16, 1976																							
6.	<u>CERTIFICATION</u>																							
6.1	Review original certifications submitted with the Plan to identify requirements for follow-up certifications																							
6.2	If required, refine the original certification forms and procedures																							
6.3	Conduct annual certifications																							
6.4	Identify any special problems relative to full Plan implementation and recommend required legislation and/or executive orders																							

Note: Tasks 5.1 through 5.6 all begin prior to March 1, 1976

1. March 16, 1976 : Initial certification completed
2. March of Each Year : Submit annual certifications
3. _____ Enact enabling legislation required to achieve full compliance with the Regulations
4. _____ State achieves full compliance with Regulations

EXHIBIT III-1: ACTION PLAN AND SCHEDULE
MONTH/YEAR OF ACTION ACTIVITY

ACTION ACTIVITY																									
No.	Description	'76 Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	'76 Dec	'77 Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	'77 Dec	Milestone Events	
6.5	Identify progress to date toward problem resolution and achievement of full compliance with the Regulations																							1. January 2, 1977 : Begin implementation of selected Standards and Goals	
6.6	Submit annual certifications and compliance comments to LEAA																								
7.	<u>STANDARDS AND GOALS</u>																								
7.1	Develop strategy for implementation of selected standards and goals relative to procedures identified in the Security and Privacy Plan																								
7.2	Develop an implementation work plan for those standards identified for implementation through administrative action																								
7.3	Enact legislation and/or issue executive orders as required to fully implement selected standards dealing with Plan compliance procedures																								

III. SCHEDULE OF MAJOR MILESTONES

This section describes the timetable and major milestone events in bringing all agencies into compliance with the Regulations. The approach used is a schedule of major action steps to be taken displayed over time which result in major milestone events. This Action Plan and Schedule is presented in Exhibit III-1.

The certification forms for each criminal justice agency who require certification provide for an estimated date for each of the relevant procedures in the Privacy and Security Plan to be fully operational in each agency (see Appendices N and O). This date is indicated whenever a criminal justice agency could make a specific commitment to operationalize the Plan's procedure; where a date is not indicated the agency was unable, at this time, to make a specific implementation commitment because of the constraints now present. A December 31, 1977 date could have been used in these constraint situations, but it will be more valuable to the Plan's implementation to know exactly where Plan implementation problems exist.

The major tasks required to implement the Privacy and Security Plan on a Statewide basis are listed in Exhibit III-1. The milestones resulting from these tasks, which are related to Privacy and Security Plan implementation, are also identified in Exhibit III-1. It is important to point out that the Exhibit III-1 Action



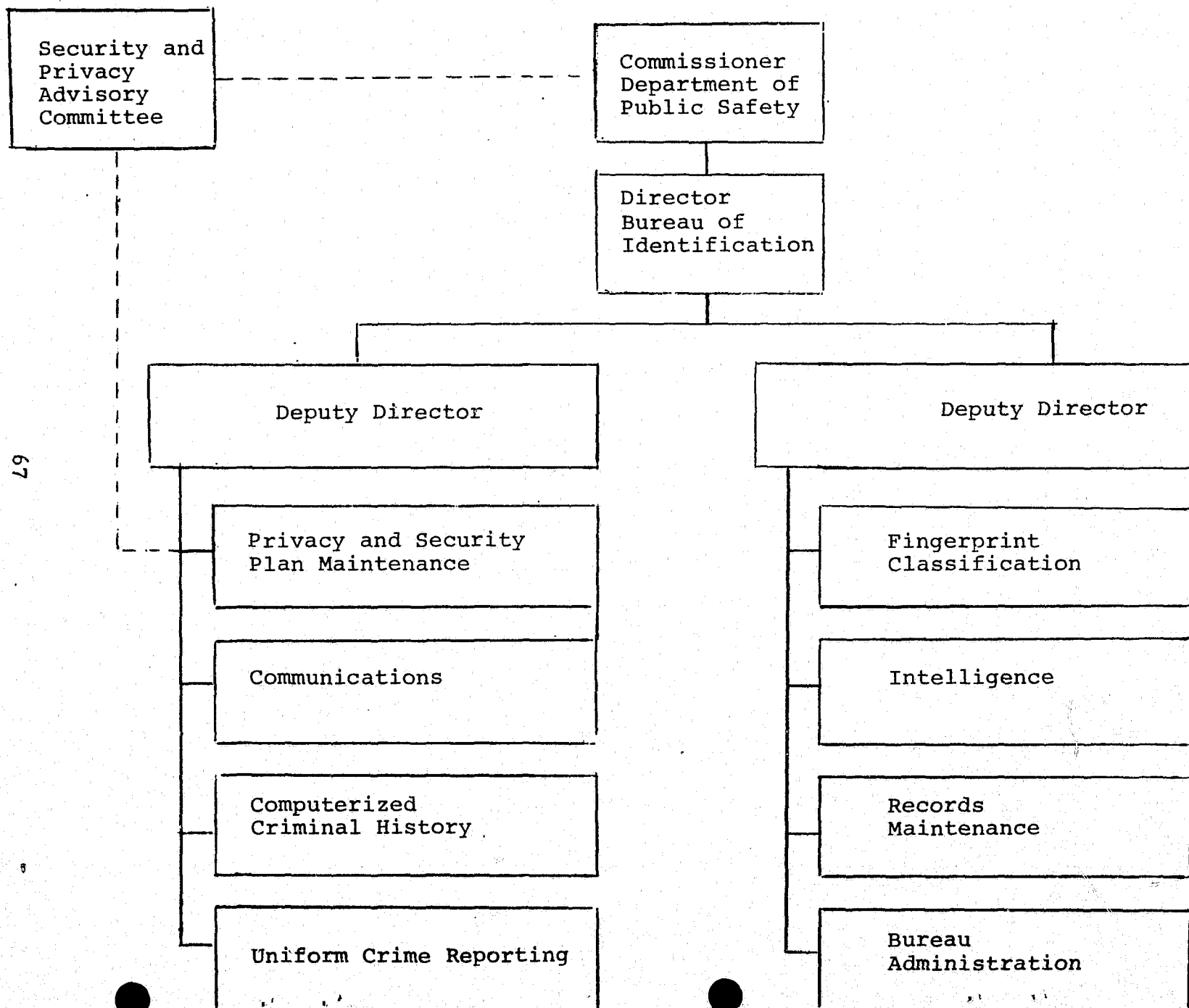
IV. RESPONSIBILITIES OF INVOLVED AGENCIES

This section summarizes the responsibilities of each State agency who is involved in some way with the implementation of the procedures set forth in this Plan. The responsibilities for Plan implementation at the local level are described in an overall context; that is, it is assumed that individual local criminal justice agencies will maintain jurisdiction (responsibility) for Plan implementation within their local agency. Also contained in this section is an overview of the strategies the State of Utah will employ to comply with the Regulations.

Several State agencies will be involved with Plan implementation and will share in the responsibility for Statewide implementation. These agencies are:

- Department of Public Safety who will be responsible for overall Plan implementation. The Utah Bureau of Identification (Central Repository) resides within the Department of Public Safety. UBI will be responsible for Statewide implementation of the Plan.
- Office of Attorney General who will establish the right of access appeal procedure and will be involved with researching and drafting of legislation required for full implementation of the Plan. They will also be involved in adjudication activities related to violations by agencies who violate provisions of the Plan and user agreements.
- Office of Legislative Analyst who will be involved in the budget process related to the Plan's implementation. They will also review all legislation related to Plan implementation.
- State Information Systems Center who will provide all State related computer services to operate the automated criminal history record information systems for the Central Repository and other State criminal justice agencies. They will also provide support and technical

EXHIBIT IV-1 : PROPOSED ORGANIZATION
FOR PRIVACY AND SECURITY PLAN IMPLEMENTATION,
OPERATION AND MAINTENANCE



personnel in the design and programming maintenance of the automated criminal history record information systems for all State criminal justice agencies.

- Security and Privacy Advisory Committee who will serve in an advisory capacity to the Commissioner of Public Safety on all matters related to the Plan's implementation. The appointing power will select representatives from all sectors of the State's criminal justice system and will invite them to serve as appointed members of the Committee. An important aspect of this Committee is the opportunity it will provide for local criminal justice agencies to have a voice in the Plan's implementation and to give adequate recognition to local criminal justice agencies' needs. In developing this Plan, it was recognized that full implementation of the Plan on a Statewide basis can only occur with full support and cooperation between the State and local criminal justice agencies.

To operationalize the Plan's procedures, additional State personnel and other resources will be required. It is proposed to reorganize the present Utah Bureau of Identification to include the needed personnel to operationalize the Plan. This proposed reorganization is shown in Exhibit IV-1. The Privacy and Security Plan maintenance unit will perform the following functions on a continuing basis:

- Develop, implement and refine specific detailed operational procedures as required by the Plan.
- Conduct annual compliance reviews to determine the degree of compliance with the Regulations and the Plan on a Statewide basis (except for the State Central Repository compliance review).
- Provide guidance and assistance to local criminal justice agencies in Plan implementation; and act in an oversight role to determine the degree of compliance with the Regulations and the Plan.
- Serve as staff to the Security and Privacy Advisory Committee.

CONTINUED

1 OF 4

- . Conduct annual certifications and compliance reviews.
- . Maintain and update the Plan.
- . Perform other functions as determined by the Director of UBI.

It is the intent of the State of Utah to operationalize the Privacy and Security Plan throughout the Utah Criminal Justice System. Instead of trying to distinguish between the small number of agencies who are specifically affected by the Regulations, all components of the Plan will be implemented (to the extent feasible) in all criminal justice agencies in the State. This is not a simple task and recognition is given to the autonomous nature of each local jurisdiction. However, attempts will be made to exhibit to these agencies the benefits to be derived through the Plan's implementation on a Statewide basis.

Implementation of the Privacy and Security Plan will have a significant cost and organizational impact at the State level, and to some extent at the local level. It is estimated that five additional personnel will be required to staff the Privacy and Security Plan Maintenance Unit in UBI. To meet this need as soon as possible, the Department of Public Safety has requested an augmentation to their 1975-76 budget to allow a manager and a secretary to be hired before May 1976. Also, one field representative has just been hired who will move into the Privacy and Security Plan Maintenance Unit when the unit becomes operational. The Department will include requests for the additional required positions in their 1976-77 budget request.

EXHIBIT IV-2: STATEWIDE PLAN IMPLEMENTATION
COST ESTIMATE DEVELOPMENT DETAILS

Criminal Justice Agency or Activity		Cost Elements Cost and Relationship In Each Agency Type (1)							Plan Implementation Cost Est.
No. (N)	Type (P _n)	c ₁	c ₂	c ₃	c ₄	c ₅	c ₆	c ₇	
29	a=Sheriffs Offices	200	70		2,200		200		\$ 77,430
154	b=Police Depts.	100	30		600		150		\$ 135,520
180	c=Justices of the Peace	50	15		100		100		\$ 47,700
15	d=City Courts	400	170		2,000		200		\$ 41,550
29	e=County Clerks	200	70		3,000		250		\$ 102,080
58	f=City and County Attorneys				100		50		\$ 8,700
7	g=State Agencies	1,000	330	1,000			1,000		\$ 23,310
1	h=State Central Repository	150,000	50,000	350,000		50,000	5,000	10,000	\$ 615,000
1	i=State Computer Center			400,000		10,000	25,000		\$ 435,000
4	j=Local Computer Centers	25,000	10,000		70,000		10,000		\$ 460,000
TOTAL COST (P)									\$1,946,290

Note: (1)

- c₁ = Computerized criminal history and disposition reporting system development and implementation
- c₂ = Delinquent disposition monitor system development and implementation
- c₃ = On-going operating expenditures required to implement specific elements of the Plan at the State level
- c₄ = On-going operating expenditures required by local criminal justice agencies to implement specific elements of the Plan
- c₅ = Printing of policy and procedures manuals and documents
- c₆ = Physical security enhancements
- c₇ = State Central Repository annual compliance review

It is difficult, if not impossible, to compute a completely accurate cost estimate to implement the Privacy and Security Plan. Estimating the costs at the local level is the most difficult; while even at the State level, cost implications are not totally clear. However, it is desirable to gain some insight into the potential cost implications and to establish an order of magnitude cost estimate. A methodology was devised to meet this desire-to-know cost information. This methodology entailed classifying criminal justice agencies by type and identifying other major types of activities at the State and local levels requiring significant expenditures. Each of the major cost elements associated with Plan implementation were then defined and associated with each type of criminal justice agency where these costs would be incurred. The cost estimate was then developed by arithmetically computing these costs by the following formula:

P = Statewide Plan Implementation Order of Magnitude Cost Estimate (through December 31, 1977 only).

$P_a \dots P_j$ = Plan Implementation Order of Magnitude Cost Estimate for all agencies or activities in each Type (a through j).

$c_1 \dots c_7$ = Estimated one-time or on-going cost basis for each cost element.

N = Number of agencies or activities in each type.

The formula for computing P is then -

$$P = P_a + \dots + P_j$$

where $P_a = N(c_1 + c_2 + c_4 + c_6)$

$$P_b = N(c_1+c_2+c_4+c_6)$$

$$P_c = N(c_1+c_2+c_4+c_6)$$

$$P_d = N(c_1+c_2+c_4+c_6)$$

$$P_e = N(c_1+c_2+c_4+c_6)$$

$$P_f = N(c_4+c_6)$$

$$P_g = N(c_1+c_2+c_3+c_6)$$

$$P_h = N(c_1+c_2+c_3+c_5+c_6+c_7)$$

$$P_i = N(c_3+c_5+c_6)$$

$$P_j = N(c_1+c_2+c_4+c_6)$$

The Statewide Plan implementation order of magnitude cost estimate of \$1,946,290.00 was then developed using this methodology. The details of the development of this cost estimate are presented in Exhibit IV-2.



APPENDICES



APPENDIX A

L.E.A.A. REGULATIONS

federal register

TUESDAY, MAY 20, 1975

WASHINGTON, D.C.

Volume 40 ■ Number 98

PART IV



DEPARTMENT OF JUSTICE

■

CRIMINAL JUSTICE INFORMATION SYSTEMS

Title 28—Judicial Administration
CHAPTER I—DEPARTMENT OF JUSTICE

[Order No. 601-75]

PART 20—CRIMINAL JUSTICE
INFORMATION SYSTEMS

This order establishes regulations governing the dissemination of criminal record and criminal history information and includes a commentary on selective sections as an appendix. Its purpose is to afford greater protection of the privacy of individuals who may be included in the records of the Federal Bureau of Investigation, criminal justice agencies receiving funds directly or indirectly from the Law Enforcement Assistance Administration, and interstate, state or local criminal justice agencies exchanging records with the FBI or these federally-funded systems. At the same time, these regulations preserve legitimate law enforcement need for access to such records.

Pursuant to the authority vested in the Attorney General by 28 U.S.C. 509, 510, 534, and Pub. L. 92-544, 86 Stat. 1115, and 5 U.S.C. 301 and 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)), this addition to Chapter I of Title 28 of the Code of Federal Regulations is issued as Part 20 by the Department of Justice to become effective June 19, 1975.

This addition is based on a notice of proposed rule making published in the FEDERAL REGISTER on February 14, 1974 (39 FR 5636). Hearings on the proposed regulations were held in Washington, D.C. in March and April and in San Francisco, California in May 1974. Approximately one hundred agencies, organizations and individuals submitted their suggestions and comments, either orally or in writing. Numerous changes have been made in the regulations as a result of the comments received.

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.
- 20.26 References.

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.

- Sec.
- 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 U.S.C. 3701, et seq.; 28 U.S.C. 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 ensure 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 U.S.C. 3701, et seq. (Act), 28 U.S.C. 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 of 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 U.S.C. 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.

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.

(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 compiled chronologically; (4) published court opinions or public judicial 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 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. 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.

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

A plan shall be submitted to LEAA by each State within 180 days of the promulgation of these 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.* Insure that dissemination of criminal history record information 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) Such other individuals and agencies which require criminal history record information to implement a statute or executive order that expressly refers to criminal conduct and contains requirements and/or exclusions expressly based upon such conduct;

(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 the 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;

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

(6) Individuals and agencies where authorized by court order or court rule.

(c) *General policies on use and dissemination.* Insure adherence to the following restrictions:

(1) Criminal history record information concerning the arrest of an individual may not be disseminated to a non-criminal justice agency or individual (except under § 20.21(b) (3), (4), (5), (6)) if an interval of one year has elapsed from the date of the arrest and no disposition of the charge has been recorded and no active prosecution of the charge is pending;

(2) Use of criminal history record information disseminated to non-criminal justice agencies under these regulations shall be limited to the purposes for which it was given and may not be disseminated further.

(3) No agency or individual shall confirm the existence or non-existence of criminal history record information for

employment or licensing checks except as provided in paragraphs (b) (1), (b) (2), and (b) (5) of this section.

(4) This paragraph sets outer limits of dissemination. It does not, however, mandate dissemination of criminal history record information to any agency or individual.

(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 non-criminal justice agencies is prohibited, unless a statute or Federal executive order 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), (4), and (6).

(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.

(f) *Security.* Insure confidentiality and security of criminal history record information by providing that wherever criminal history record information is collected, stored, or disseminated, a criminal justice agency shall—

(1) Institute where computerized data processing is employed effective and technologically advanced software and hardware designs to prevent unauthorized access to such information;

(2) Assure that where computerized data processing is employed, the hardware, including processor, communications control, and storage device, to be utilized for the handling of criminal history record information is dedicated to purposes related to the administration of criminal justice;

(3) Have authority to set and enforce policy concerning computer operations;

(4) Have power to veto for legitimate security purposes which personnel can be permitted to work in a defined area where such information is stored, collected, or disseminated;

(5) Select and supervise all personnel authorized to have direct access to such information;

(6) Assure that an individual or agency authorized direct access is administratively held 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 accesses, disclosure, or dissemination;

(7) Institute procedures to reasonably protect any central repository of criminal history record information from unauthorized access, theft, sabotage, fire, flood, wind, or other natural or man-made disasters;

(8) Provide that each employee working with or having access to criminal history record information should be made

familiar with the substance and intent of these regulations; and

(9) Provide that direct access to criminal history records information shall be available only to authorized officers or employees of a criminal justice agency.

(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 each 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 up-

grade such capability to meet the requirements of these regulations; and

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

§ 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, except that a State, upon written application and good cause, may be allowed an additional period of time to implement § 20.21(f)(2). Certification shall be submitted in December of each year to LEAA until such complete compliance. The yearly certification shall update the information provided under § 20.21.

§ 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.

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, non-specific 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.

APPENDIX—COMMENTARY ON SELECTED SECTIONS OF THE REGULATIONS ON CRIMINAL HISTORY RECORD INFORMATION SYSTEMS

Subpart A—§ 20.3(b). The definition of criminal history record information is intended to include the basic offender-based transaction statistics/computerized criminal history (OBTS/CCH) data elements. If notations of an arrest, disposition, or other formal criminal justice transactions occur in records other than the traditional "rap sheet" such as arrest reports, any criminal history record information contained in such reports comes under the definition of this subsection.

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

§ 20.3(c). The definitions of criminal justice agency and administration of criminal justice of 20.3(c) (d) must be considered together. Included as criminal justice agencies would be traditional police, courts, and corrections agencies as well as subunits of non-criminal justice agencies performing a function of the administration of criminal justice pursuant to Federal or State statute or executive order. The above subunits of non-criminal justice agencies would include for example, the Office of Investigation of the U.S. Department of Agriculture which has as its principal function the collection of evidence for criminal prosecutions of fraud. Also included under the definition of criminal justice agency are umbrella-type administrative agencies supplying criminal history information services such as New York's Division of Criminal Justice Services.

§ 20.3(e). Disposition is a key concept in the section 524(b) of the Act and in § 20.21 (a) (1) and § 20.21(b) (2). It, therefore, is defined in some detail. The specific dispositions listed in this subsection are examples only and are not to be construed as excluding other unspecified transactions concluding criminal proceedings within a particular agency.

Subpart B—§ 20.20(a). These regulations apply to criminal justice agencies receiving Safe Streets funds for manual or automated systems subsequent to July 1, 1973. In the hearings on the regulations, a number of those testifying challenged LEAA's authority to promulgate regulations for manual systems by contending that section 524(b) of the Act governs criminal history information contained in automated systems.

The intent of section 524(b), however, would be subverted by only regulating automated systems. Any agency that wished to circumvent the regulations would be able to create duplicate manual files for purposes contrary to the letter and spirit of the regulations.

Regulations of manual systems, therefore, is authorized by section 524(b) when coupled with Section 501 of the Act which authorizes the Administration to establish rules and regulations "necessary to the exercise of its functions * * *."

The Act clearly applies to all criminal history record information collected, stored, or disseminated with LEAA support subsequent to July 1, 1973.

§ 20.20(b)(c). Section 20.20(b)(c) exempts from regulations certain types of records vital to the apprehension of fugitives, freedom of the press, and the public's right to know.

Section 20.20(b)(11) attempts to deal with the problem of computerized police blotters. In some local jurisdictions, it is apparently possible for private individuals and/or newsmen upon submission of a specific name to obtain through a computer search of the blotter a history of a person's arrests. Such files create a partial criminal history data bank potentially damaging to individual privacy, especially since they do not contain final dispositions. By requiring that such records be accessed solely on a chronological basis, the regulations limit inquiries to specific time periods and discourage general fishing expeditions into a person's private life.

Subsection 20.20(c) recognizes that announcements of ongoing developments in the criminal justice process should not be precluded from public disclosure. Thus announcements of arrest, convictions, new developments in the course of an investigation may be made within a few days of their occurrence. It is also permissible for a criminal justice agency to confirm certain matters of public record information upon specific inquiry. Thus, if a question is raised: "Was X arrested by your agency on January 3, 1952" and this can be confirmed or denied by looking at one of the records enumerated in subsection (b) above, then the criminal agency may respond to the inquiry.

§ 20.21. Since privacy and security considerations are too complex to be dealt with overnight, the regulations require a State plan to assure orderly progress toward the objectives of the Act. In response to requests of those testifying on the draft regulations, the deadline for submission of the plan was set at 180 days. The kind of planning document anticipated would be much more concise than, for example, the State's criminal justice comprehensive plan.

The regulations deliberately refrain from specifying who within a State should be responsible for preparing the plan. This specific determination should be made by the Governor.

§ 20.21(a)(1). Section 524(b) of the Act requires that LEAA insure criminal history information be current and that, to the maximum extent feasible, it contain disposition as well as current data.

It is, however, economically and administratively impractical to maintain complete criminal histories at the local level. Arrangements for local police departments to keep track of dispositions by agencies outside of the local jurisdictions generally do not exist. It would, moreover, be bad public policy to encourage such arrangements since it would result in an expensive duplication of files.

The alternatives to locally kept criminal histories are records maintained by a central State repository. A central State repository is a State agency having the function pursuant to statute or executive order of maintaining comprehensive statewide criminal history record information files. Ultimately, through automatic data processing the State level will have the capability to handle all requests for in-State criminal history information.

Section 20.21(a)(1) is written with a centralized State criminal history repository in mind. The first sentence of the subsection states that complete records should be retained at a central State repository. The word "should" is permissive; it suggests but does not mandate a central State repository.

The regulations do require that States establish procedures for State and local criminal justice agencies to query central State repositories wherever they exist. Such procedures are intended to insure that the most current criminal justice information is used.

As a minimum, criminal justice agencies subject to these regulations must make inquiries of central State repositories whenever the repository is capable of meeting the user's request within a reasonable time. Presently, comprehensive records of an individual's transactions within a State are maintained in manual files at the State level, if at all. It is probably unrealistic to expect manual systems to be able immediately to meet many rapid-access needs of police and prosecutors. On the other hand, queries of the State central repository for most non-criminal justice purposes probably can and should be made prior to dissemination of criminal history record information.

§ 20.21(b). The limitations on dissemination in this subsection are essential to fulfill the mandate of section 524(b) of the Act which requires the Administration to assure that the "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." The categories for dissemination established in this section reflect suggestions by hearing witnesses and respondents submitting written commentary.

§ 20.21(b)(2). This subsection is intended to permit public or private agencies to have access to criminal history record information where a statute or executive order:

(1) Denies employment, licensing, or other civil rights and privileges to persons convicted of a crime;

(2) Requires a criminal record check prior to employment, licensing, etc.

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

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

§ 20.21(b)(3). This subsection would permit private agencies such as the Vera Institute to receive criminal histories where they perform a necessary administration of justice function such as pretrial release. Private consulting firms which commonly assist criminal justice agencies in information systems development would also be included here.

§ 20.21(b)(4). Under this subsection, any good faith researchers including private individuals would be permitted to use criminal history record information for research purposes. As with the agencies designated in § 20.21(b)(3) researchers would be bound by an agreement with the disseminating criminal justice agency and would, of course, be subject to the sanctions of the Act.

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

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

"Except as provided by Federal law other than this title, no officer or employee of the Federal Government, nor any recipient of assistance under the provisions of this title shall use or reveal any research or statistical information furnished under this title by any person and identifiable to any specific private person for any purpose other than the purpose for which it was obtained in accordance with this title. Copies of such information shall be immune from legal process, and shall not, without the consent of the person furnishing such information, be admitted as evidence or used for any purpose in any action, suit, or other judicial or administrative proceedings."

LEAA anticipates issuing regulations pursuant to Section 524(a) as soon as possible.

§ 20.21(b)(5). Dissemination under this section would be permitted not only in cases of investigations of employment suitability, but also investigations relating to clearance of individuals for access to information which is classified pursuant to Executive Order 11652.

§ 20.21(c)(1). "Active prosecution pending" would mean, for example, that the case is still actively in process, the first step such as an arraignment has been taken and the case docketed for court trial. This term is not intended to include any treatment alternative-type program which might defer prosecution to a later date. Such a deferral prosecution is a disposition which should be entered on the record.

§ 20.21(c)(3). Presently some employers are circumventing State and local dissemination restrictions by requesting applicants to obtain an official certification of no criminal record. An employer's request under the above circumstances gives the applicant the unenviable choice of invasion of his privacy or loss of possible job opportunities. Under this subsection routine certifications of no record would no longer be permitted. In extraordinary circumstances, however, an individual could obtain a court order permitting such a certification.

§ 20.21(c)(4). The language of this subsection leaves to the States the question of who among the agencies and individuals listed in § 20.21(b) shall actually receive criminal records. Under these regulations a State could place a total ban on dissemination if it so wished.

§ 20.21(d). Non-criminal justice agencies will not be able to receive records of juveniles unless the language or statute or Federal executive order specifies that juvenile records shall be available for dissemination. Perhaps the most controversial part of this subsection is that it denies access to records of juveniles by Federal agencies conducting background investigations for eligibility to classified information under existing legal authority.

§ 20.21(e). Since it would be too costly to audit each criminal justice agency in most States (Wisconsin, for example, has 1075 criminal justice agencies) random audits of a "representative sample" of agencies are the next best alternative. The term "representative sample" is used to insure that audits do not simply focus on certain types of agencies.

§ 20.21(f)(2). In the short run, dedication will probably mean greater costs for State and local governments. How great such costs might be is dependent upon the rapidly advancing state of computer technology. So that there will be no serious hardship on States and localities as a result of this requirement, § 20.23 provides that additional time will be allowed to implement the dedication requirement. For example, where local systems now in place contain criminal history information of only that State, used purely for intrastate purposes, in a shared environment, consideration will be given to

granting extensions of time under this provision.

§ 20.21(f) (5), (8). "Direct access" means that any non-criminal agency authorized to receive criminal justice data must go through a criminal justice agency to obtain information.

§ 20.21(g) (1). A "challenge" under this section is an oral or written contention by an individual that his record is inaccurate or incomplete; it would require him to give a correct version of his record and explain why he believes his version to be correct. While an individual should have access to his record for review, a copy of the record should ordinarily only be given when it is clearly established that it is necessary for the purpose of challenge.

The drafters of the subsection expressly rejected a suggestion that would have called for a satisfactory verification of identity by fingerprint comparison. It was felt that states ought to be free to determine other means of identity verification.

§ 20.21(g) (5). Not every agency will have done this in the past, but henceforth adequate records including those required under § 20.21(e) must be kept so that notification can be made.

§ 20.21(g) (6). This section emphasizes that the right to access and review extends only to criminal history information and does not include other information such as intelligence or treatment data.

§ 20.22(a). The purpose for the certification requirement is to initiate immediate compliance with these regulations wherever possible. The term "maximum extent feasible" acknowledges that there are some areas such as the completeness requirement which create complex legislative and financial problems.

NOTE: In preparing the plans required by these regulations, States should look for guidance to the following documents: National Advisory Commission on Criminal Justice Standards and Goals, Report on the Criminal Justice System; Project SEARCH: Security and Privacy Considerations in Criminal History Information Systems, Technical Report #2; Project SEARCH: A Model State Act for Criminal Offender Record Information, Technical Memorandum #3; and Project SEARCH: Model Administrative Regulations for Criminal Offender Record Information, Technical Memorandum #4.

Subpart C—§20.31. Defines the criminal history record information system operated by the Federal Bureau of Investigation. Each state having a record in the Computerized Criminal History (CCH) file must have a fingerprint card on file in the FBI Identification Division to support the CCH record concerning the individual.

Paragraph b is not intended to limit the identification services presently performed

by the FBI for Federal, state and local agencies.

§ 20.32. The grandfather clause contained in the third paragraph of this Section is designed, from a practical standpoint, to eliminate the necessity of deleting from the FBI's massive files the non-includable offenses which were stored prior to February, 1973.

In the event a person is charged in court with a serious or significant offense arising out of an arrest involving a non-includable offense, the non-includable offense will appear in the arrest segment of the CCH record.

§ 20.33. Incorporates the provisions of a regulation issued by the FBI on June 26, 1974, limiting dissemination of arrest information not accompanied by disposition information outside the Federal government for non-criminal justice purposes. This regulation is cited in 28 CFR 50.12.

§ 20.34. The procedures by which an individual may obtain a copy of his manual identification record are particularized in 28 CFR 16.30-34.

The procedures by which an individual may obtain a copy of his Computerized Criminal History record are as follows:

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

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

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

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

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

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

§ 20.36. This section refers to the requirements for obtaining direct access to the CCH file. One of the requirements is that hardware, including processor, communications control and storage devices, to be utilized for the handling of criminal history data must be dedicated to the criminal justice function.

§ 20.37. The 120-day requirement in this section allows 30 days more than the similar provision in Subpart B in order to allow for processing time which may be needed by the states before forwarding the disposition to the FBI.

[FR Doc.75-13197 Filed 5-19-75;8:45 am]

[Order No. 602-75]

PART 50—STATEMENTS OF POLICY

Release of Information by Personnel of the Department of Justice Relating to Criminal and Civil Proceedings

This order amends the Department of Justice guidelines concerning release of information by personnel of the Department of Justice relating to criminal and civil proceedings by deleting the provision permitting disclosure of criminal history record information on request.

By virtue of the authority vested in me as Attorney General of the United States, § 50.2(b) (4) of Chapter I, Title 28 of the Code of Federal Regulations is amended to read as follows:

§ 50.2 Release of information by personnel of the Department of Justice relating to criminal and civil proceedings.

* * * * *

(4) Personnel of the Department shall not disseminate any information concerning a defendant's prior criminal record.

* * * * *

MAY 15, 1975.

EDWARD H. LEVI,
Attorney General.

[FR Doc.75-13198 Filed 5-19-75;8:45 am]

APPENDIX B

UTAH CODE ANNOTATED 1953

TITLE 77, CHAPTER 59



TITLE 77, CHAPTER 59
UTAH CODE ANNOTATED 1953

CRIMINAL IDENTIFICATION

77-59-3 Commissioner--Compensation--Assistants

The state bureau of criminal identification shall be under the supervision and control of the commissioner of public safety. The commissioner shall receive no extra compensation or salary as head of the bureau but shall be reimbursed for expenses actually and necessarily incurred in the performance of his duties as supervisor of the bureau. The commissioner shall appoint such deputies, inspectors, examiners, clerical workers and other employees as may be required to properly discharge the duties of the bureau which employees and assistants shall serve at the pleasure of the commissioner and whose salaries shall be fixed in accordance with standards adopted by the department of finance.

77-59-4 Offices at Capitol

Suitable offices for the bureau shall be provided in the state capitol and its board of managers may equip and furnish said offices.

77-59-5 General Duties and Functions of Bureau and Employees.

The bureau shall procure and file for record, plates, photographs, outline pictures, descriptions, information, statistics, fingerprints and measurements, wherever procurable of persons who are fugitives from justice, wanted or missing or who have been or shall hereafter be convicted of felony or an indictable misdemeanor under the laws of any state or of the United States and of all well-known and habitual criminals, and file the same with information and descriptions received by it in the course of the administration of the bureau; and it shall make a complete and systematic record and index of the same, providing thereby a method of convenient consultation and comparison. So far as practicable such records shall coincide in form with those of the Federal Bureau of Investigation in order to facilitate interchange of records. It shall be the further duty of the employees of the department to prevent and detect crime, to apprehend criminals and to enforce the criminal laws of the state and to perform such other related duties as may be imposed upon them by the legislature.

77-59-6 System and Means of Identification

The commissioner shall adopt rules prescribing systems of identification, known as the fingerprint system, or any system of measurements that may from time to time be adopted or used to facilitate the enforcement of the law in the various law enforcement agencies throughout the nation; and shall use its discretion in improving the methods of identification and in adopting systems of measurements, processes, operation, plates, photographs and descriptions of all persons confined in penal institutions of the state, in accordance with approved systems of identification of criminals.

77-59-7 System of Recording-Visitation of Secure Data

The bureau shall adopt a system of recording, with necessary indexes, and keep complete records of all reports filed with it, and of all property stolen, lost or found and from time to time shall improve such records so as to provide for the further identification of persons guilty of crime. The commissioner and persons designated by him are authorized to call upon any of the law enforcement officers of the state, the warden of the state prison and the keeper of any jail or any penal institution which may hereafter be established to furnish information which will aid in making up the records required to be kept; and all officers called upon are required to furnish the information requested by the bureau or the persons designated by it. The commissioner and all persons acting under him are hereby given authority, upon showing credentials, to enter any jail, state prison or other place of confinement maintained by the state or any subdivision thereof to take or cause to be taken fingerprints or photographs, and make investigation relative to any person confined therein, for the purpose of obtaining information which will lead to the identification of criminals; and every person, who had charge of custody of public records or documents, from which it may reasonably be supposed that information, described in sections 77-59-9, 77-59-11, 77-59-12 and 77-59-13 hereof, can be obtained shall grant access thereto to any employee of the bureau upon written authorization by the director or shall produce such records or documents for the inspection and examination of such employee.

77-59-8 Commissioner-Powers and Duties-Appointment, Promotion and Removal of Employees-Bonds.

The Commissioner shall, and within the limits of any appropriation made for such purpose, appoint and promote such employees to the ranks, grades and positions as are deemed necessary for the efficient administration of the bureau under the

provisions of this act. He shall have authority to formulate, put into effect, alter and revise such regulations for the administration of the bureau as seem expedient, and may discharge, demote or temporarily suspend an employee for misconduct, incompetence or failure to perform his duties or to properly observe rules and regulations of the bureau and shall have authority to determine the conditions of bonds to be required of employees in such amounts as shall be prescribed by the state department of finance.

77-59-9 Duty of Sheriff and Police Chiefs to Transmit Data to Bureau.

Every sheriff and every chief police officer of the state and of any local government unit shall transmit to the bureau, so far as available, as provided in section 77-59-14 hereof:

(a) The names, fingerprints, photographs, and such other data as the director may from time to time prescribe of all persons arrested for, or suspected of:

(1) An indictable offense, or such nonindictable offense as is or may hereafter be, included in the compilations of the division of investigation of the U. S. department of justice;

(2) Being fugitive from justice;

(3) Being vagrants;

(4) Being habitual users of narcotics, or other habit-forming drugs;

(5) Being in possession of stolen goods or of goods believed to have been stolen; and

(6) Being in possession of illegal or illegally carried weapons or in possession of burglar's tools, tools for the defacing or altering of the numbers of automobiles, automobile parts, automobile engines, or automobile engine parts; or illegally in possession of tools, supplies, or other articles used in the manufacture or alteration of money or bank notes or in any wise making counterfeit thereof; or illegally in possession of highpower explosives, infernal machines, bombs, or other contrivances reasonably believed by the arresting person to be intended to be used for unlawful purposes.

(b) The fingerprints, photographs, and other data prescribed by the director concerning unidentified dead persons, amnesia victims and in so far as available, missing persons.

(c) A record of the indictable offenses and of such nonindictable offenses as are, or may hereafter be, included in the compilation of the Federal Bureau of Investigation, and which are committed within the jurisdiction of the reporting officer, including a statement of the facts of the offense, and so far as known, a description

of the offender, the method of operation, the official action taken and such other information as the director may require.

(d) Copies of such reports as are now required by law to be made or as may hereafter be so required, and as shall be prescribed by the director, to be made by pawnshops, second-hand dealers, and dealers in weapons.

(e) Lists of stolen automobiles and of automobiles recovered with their engine and serial numbers, descriptions and other identification data, and lists of such other classes of stolen property as the director shall prescribe.

77-59-10 Powers of Commissioner and Employees-Extent of Powers.

The commissioner and such of the employees as shall be deputized by him for the purpose shall be vested with the power of peace officers and may exercise their powers as such throughout the state, with the exception of the power to serve civil processes. They shall have, in any part of the state, the same powers and respect to criminal matters and the enforcement of the law relating thereto, as sheriffs and police officers have in their respective jurisdictions and shall have all the immunities and matters of defense now available and hereafter made available to sheriffs and police officers in any suit brought against them in consequence of acts done in the course of their employment; provided, however, that they shall in no wise usurp the powers of the local police and sheriffs, but shall cooperate with them and shall be available when possible to respond to requests from the police and sheriffs to aid in the detection, apprehension and prosecution of criminals; nor shall they in no wise supersede the authority of the local police units unless given special order under the authority of the governor.

77-59-11 Duties of Court Clerks, Judges and Justices-Transmission of Data

Every clerk of a court having original or appellate jurisdiction over indictable offenses, or if there be no clerk, every judge or justice of such court, shall transmit to the bureau, as provided in section 77-59-14 hereof, such statistics and information as the director shall prescribe regarding indictments and information filed in such court and the disposition made of them, pleas, convictions, acquittals, probations granted or denied and any other disposition of criminal proceeding made in such court.

77-59-12 Duties of Coroners and Justices of the Peace.

Every coroner, or justice of the peace shall transmit to the bureau, as provided in section 77-59-14 hereof, such statistics and information as the

commissioner shall prescribe, regarding autopsies performed, inquests held, and verdicts rendered.

77-59-13 Penal Institutions-Transmission of Data.

Every person in responsible charge (of) an institution to which there are committed persons convicted of crime or juvenile delinquency or declared to be criminally insane or to be feeble-minded, and every probate officer shall transmit to the bureau as contained in section 77-59-14 hereof:

(a) The names, fingerprints, photographs and other (data) prescribed by the director of all persons who are received in such institutions for the violation of an indictable offense and of all persons placed on probation for such an offense so far as such information is available.

(b) Full reports of all transfers to or from such institutions, paroles granted and revoked, discharges from such institution or paroles, commutations of sentence and pardons of all persons described in section (a) of this section.

77-59-14 Time and Manner of Transmission of Information or Data.

The officers and officials described in Sections 77-59-9, 77-59-11, 77-59-12 and 77-59-13, hereof, shall furnish to the bureau the information and reports specified in sections 77-59-9, 77-59-11, 77-59-12 and 77-59-13, hereof, at or within such times or periods as shall be designated, on forms to be prescribed by the commissioner (and conforming Where Appropriate, to the uniform system of criminal statistics of the Federal Bureau of Investigation) and supplied by the bureau to the Said officers, and in such number of copies as the commissioner may require.

77-59-15 Report on Persons Released from Penal Institutions.

It is hereby made the duty of the warden or keeper of the state prison or such other penal institutions as the state may hereinafter establish, when called upon to do so, to furnish a report monthly or oftener, as may be deemed necessary by the bureau, of all persons released therefrom during the preceding month, indicating how and when released and also furnish a full length photograph of each such persons released, the same to be taken immediately prior to date of such release.

77-59-16 Facilities to be Furnished Officers.

It is further provided that any and all governing boards or commissions of each city, town, county or penal institution of the state are hereby required to

furnish the officers with the necessary supplies and equipment to properly perform their duties as prescribed in this act, also, the necessary supplies and equipment to properly compile and preserve all fingerprint cards and original records.

77-59-17 Duty of Bureau of Criminal Identification and Investigation-Filing data, fingerprints for parents.

The bureau shall accept and file the names, fingerprints, photographs, and other personal identification data submitted voluntarily by individuals or submitted by parents on behalf of their children for the purpose of securing a more certain and easy identification in case of death, injury, loss of memory, or change of appearance of such person. Any law enforcement officer mentioned in this act shall, when requested so to do by any citizen of the state, take without cost to the citizen, at least two sets of fingerprints of such citizen and forward one copy to the state bureau and one to the Federal Bureau of Investigation, Washington, D. C. It is further provided that such fingerprints of citizens, filed for personal identification shall not be used for any other purpose except under order of a court of competent jurisdiction.

77-59-18 Furnishing Information to Officers and Judges.

Upon application the bureau shall furnish a copy of all information available pertaining to the identification and history of any person or persons of whom the bureau has a criminal record or any other information:

(1) To any sheriff or chief police officer of the state or of any local government unit, or to any officer of similar rank and description of any other state, or of the United States, or of any jurisdiction thereof, or of any foreign country, or

(2) To the superintendent or chief officer of any bureau similar in nature to this bureau in any other state or in the United States or in any jurisdiction thereof, or in any foreign country, or

(3) To the prosecuting attorney in any court of this state in which such a person is being tried for any offense, or

(4) To the judge in any court of this state in which such a person is so being tried.

77-59-19 Duty with Respect to Informers.

If any officer or official described in section hereof, shall transmit to the Bureau of Identification data of any unidentified deceased or injured person or of any person suffering from loss of memory, the bureau shall furnish to such

officer or official any information available pertaining to the identification of such person.

77-59-20 Application for Information-Necessity for.

Although no application for information has been made to the bureau as provided in section 77-59-18, hereof, the bureau may transmit such information as the commissioner shall in his discretion designate to such persons as are authorized by section 77-59-18 hereof, to make application for it.

77-59-21 Cooperation with Bureaus of Other States and Federal Bureaus.

The bureau shall cooperate with the Federal bureau and with similar bureaus in other states and other cities toward the end of developing and carrying on a complete interstate, national and international system of criminal identification, investigation and statistics and further toward attaining this end, every sheriff and every chief police officer of the state and of any local government unit shall speedily transmit directly to the Federal Bureau of Investigation duplicate copies of all the information and data which that division shall from time to time request the commissioner to collect for it.

77-59-22 Duty to Assist Other Public Officers.

The commissioner may on request of any sheriff or chief police officer of any local government unit in the state assist such officer:

- (1) in the establishment of local identification records systems;
- (2) in investigating the circumstances of any crime and in the identification, apprehension and conviction of the perpetrator or perpetrators thereof, and for this purpose may detail such employee or employees of the bureau, for such length of time as the commissioner deems fit; and

- (3) without such request the commissioner shall at the direction of the governor, detail such employee or employees, for such time as the governor may deem fit, to investigate any crime within this state for the purpose of identifying apprehending and convicting the perpetrator or perpetrators thereof.

77-59-23 Laboratory Facilities.

To the end that he may be able to furnish the assistance and aid specified in section 77-59-22 hereof, the commissioner may provide in the bureau and maintain therein scientific crime detection laboratory facilities.

77-59-24 Communication System.

For the purpose of expediting local, state, national and international efforts in the detection and apprehension of criminals, the bureau may operate and coordinate such communication systems as may be required in the normal conduct of its duties as herein set forth.

77-59-25 Instruction and Assistance to Peace Officers.

The commissioner shall so far as feasible afford instruction and assistance to peace officers in the operation of their local identification, investigation and record systems, so as to assure coordination with the system of identification conducted by the bureau and the Federal Bureau of Investigation.

77-59-26 Records and Files of Bureau-Admissibility in Evidence.

Any copy of a record, picture, photograph, fingerprint or any other paper or document in the files of the bureau, certified by the commissioner to be a true copy of the original, shall be admissible in evidence in any court of this state in the same manner as the original might be.

77-59-27 Access to-Secrecy of.

Only employees of the bureau and persons specifically authorized by the commissioner shall have access to the files or records of the bureau. No such file or record or information shall be disclosed by any employee of the bureau except to officials as hereinbefore provided and except as may be deemed necessary by the commissioner in the apprehension or trial of persons accused of offenses or in the identifications of persons or of property.

77-59-28 Rewards-Rights of Employees of Bureau.

No reward offered for the apprehension or conviction of any person or for the recovery of any property may be accepted by any employee of the bureau, but any reward to which such employee would otherwise be entitled shall be received by the bureau and credited to its budget.

77-59-29 Authority of Officials and Employees to take Fingerprints, Photographs.

To the end that the officers and officials described in sections 77-59-9, 77-59-11, 77-59-12, and 77-59-13 hereof, may be enabled to transmit the reports required by them in the said sections, such officers and officials shall have the authority and duty to take or cause to be taken, fingerprints, photographs, and other data of the persons described in the said sections 77-59-9, 77-59-11, 77-59-12

and 77-59-13. A like authority shall be had by employees of the bureau who are authorized to enter any institution under the provisions of section 77-59-7 hereof, as to persons confined in such institutions.

77-59-30 Removal of Officers-Misfeasance or Nonfeasance.

Any person who neglects or refuses to make any report lawfully required of him under the provisions of this act, or to do or perform any other act so required to be done or performed by him, or who shall hinder or prevent another from doing an act so required to be done by that other, shall be subject to removal from office.

77-59-31 Crimes and Penalties-Violation of Act.

Any person who shall wilfully give any false information or wilfully withhold information in any report lawfully required of him under the provisions of this act, or who shall remove, destroy, alter, or mutilate any file or record of the bureau, shall be guilty of a misdemeanor, and such person shall, upon conviction thereof, be punished by a fine of not more than \$----or by imprisonment in the county jail for not more than ___ days or by both such fine and imprisonment in the discretion of the court.

77-59-32 Construction of Act.

This act shall be liberally construed to the end that offenders may be promptly and certainly identified, apprehended and prosecuted.

Section 3. Duties of Board and Director Transferred to Commissioner.

Whenever any existing or continuing law names or refers to the board of managers, or the director of the bureau of criminal identification, it shall be construed to refer to the commissioner of public safety.

APPENDIX C

UTAH ARREST AND COURT DISPOSITION REPORT

IDENTIFICATION SECTION

NAME: LAST FIRST MIDDLE	ARRESTING AGENCY ID	CDR NO.
ALIASES: LAST FIRST MIDDLE		UBI NO.
RESIDENCE:	CONTRIBUTING AGENCY ID	FBI NO.
		YOUR NO.

DATE OF BIRTH	PLACE OF BIRTH	SEX	RACE	SCARS, MARKS, TATTOOS AND AMPUTATIONS
---------------	----------------	-----	------	---------------------------------------

HAIR	EYES	HGT.	WGT.	WARRANT NO.	DATE OF ARREST	NCIC ID NEXT APPEAR
------	------	------	------	-------------	----------------	---------------------

CG NO.	INITIAL CHARGE DESCRIPTION OR STATUTE CITATION	NCIC CODE	DATE OF OFFENSE	ARREST DISP. CODE	ARREST DISP. DATE	BAIL/BOND SET		
						YES	NO	AMOUNT
1								
2								
3								
4								
5								

Signature of Official Taking Prints	Date Print Taken	Signature of Person Fingerprinted
-------------------------------------	------------------	-----------------------------------

--	--	--	--	--

1. RIGHT THUMB	2. RIGHT INDEX	3. RIGHT MIDDLE	4. RIGHT RING	5. RIGHT LITTLE

6. LEFT THUMB	7. LEFT INDEX	8. LEFT MIDDLE	9. LEFT RING	10. LEFT LITTLE

LEFT FOUR FINGERS TAKEN SIMULTANEOUSLY	LEFT THUMB	RIGHT THUMB	RIGHT FOUR FINGERS TAKEN SIMULTANEOUSLY

DEPARTMENT OF PUBLIC SAFETY
UTAH ARREST AND COURT DISPOSITION REPORT

IDENTIFICATION SECTION												
NAME: LAST FIRST MIDDLE						ARRESTING AGENCY ID			CDR NO.			
ALIASES: LAST FIRST MIDDLE									UBI NO			
RESIDENCE:						CONTRIBUTING AGENCY ID			FBI NO.			
									YOUR NO			
DATE OF BIRTH			PLACE OF BIRTH			SEX	RACE	SCARS, MARKS, TATTOOS AND AMPUTATIONS				
HAIR	EYES	HGT.	WGT.	WARRANT NO.	DATE OF ARREST	NCIC ID NEXT APPEAR						
CG NO.	INITIAL CHARGE DESCRIPTION OR STATUTE CITATION					NCIC CODE	DATE OF OFFENSE	ARREST DISP. CODE	ARREST DISP. DATE	BAIL/BOND SET YES	BAIL/BOND SET NO	BAIL/BOND SET AMOUNT
1												
2												
3												
4												
5												

COURT SECTION											
NCIC COURT CODE				CASE NO. (DOCKET)		DATE TRIAL BEGINS		DATE TRIAL ENDS		TYPE TRIAL	
										JURY NON JURY	
TYPE COUNSEL				SENTENCE DATE		SENTENCE		AGENCY REFERRED TO		REMARKS	
TYPE ACTION		NCIC AGENCY CODE		FILING DATE		TYPE FILING					
<input type="checkbox"/> TRIAL <input type="checkbox"/> APPEAL						<input type="checkbox"/> INFORMATION <input type="checkbox"/> GRAND JURY INDICTMENT <input type="checkbox"/> OTHER					
CG NO.	FINAL CHARGE DESCRIPTION OR STATUTE CITATION					NCIC CODE	PLEA AT TRIAL	CONVICTED OFFENSE	DISPOSITION CODE	DISPOSITION DATE	SENTENCE TYPE
1											
2											
3											
4											
5											

TO: STATE BUREAU OF CRIMINAL IDENTIFICATION • 300 STATE OFFICE BLDG • SALT LAKE CITY, UTAH 84114

PRELIMINARY HEARING SECTION											
NAME: LAST FIRST MIDDLE						CDR NO.					
NCIC AGENCY CODE			DATE HEARING BEGINS		DATE HEARING ENDS		TYPE COUNSEL				
							<input type="checkbox"/> PRIVATE <input type="checkbox"/> COURT APPOINTED <input type="checkbox"/> PUBLIC DEFENDER <input type="checkbox"/> SELF <input type="checkbox"/> OTHER				
AGENCY REFERRED TO			REMARKS								
CG NO.	INITIAL CHARGE DESCRIPTION OR STATUTE CITATION					NCIC CODE	RESULTS OF HEARING				NEW NCIC CODE
1							<input type="checkbox"/> DISMISSED <input type="checkbox"/> REDUCED TO MISDEMEANOR <input type="checkbox"/> BOUND OVER <input type="checkbox"/> REFILED AS MISDEMEANOR				
2							<input type="checkbox"/> DISMISSED <input type="checkbox"/> REDUCED TO MISDEMEANOR <input type="checkbox"/> BOUND OVER <input type="checkbox"/> REFILED AS MISDEMEANOR				
3							<input type="checkbox"/> DISMISSED <input type="checkbox"/> REDUCED TO MISDEMEANOR <input type="checkbox"/> BOUND OVER <input type="checkbox"/> REFILED AS MISDEMEANOR				
4							<input type="checkbox"/> DISMISSED <input type="checkbox"/> REDUCED TO MISDEMEANOR <input type="checkbox"/> BOUND OVER <input type="checkbox"/> REFILED AS MISDEMEANOR				
5							<input type="checkbox"/> DISMISSED <input type="checkbox"/> REDUCED TO MISDEMEANOR <input type="checkbox"/> BOUND OVER <input type="checkbox"/> REFILED AS MISDEMEANOR				

TO: STATE BUREAU OF CRIMINAL IDENTIFICATION • 300 STATE OFFICE BLDG. • SALT LAKE CITY, UTAH 84114

ARRAIGNMENT SECTION													
NAME: LAST FIRST MIDDLE						CDR NO.							
NCIC AGENCY CODE		CASE NO.		ARRAIGNMENT DATE		TYPE CHARGE		TYPE ACTION		AGENCY REFERRED TO			
						<input type="checkbox"/> FELONY <input type="checkbox"/> MISDEMEANOR		<input type="checkbox"/> TRIAL <input type="checkbox"/> APPEAL					
CG NO.	INITIAL CHARGE DESCRIPTION OR STATUTE CITATION					NCIC CODE	PLEA	PROSECUTOR DISP.	RELEASE ACTION CODE	RELEASE ACTION DATE	BAIL/BOND SET YES	BAIL/BOND SET NO	BAIL/BOND SET AMOUNT
1							<input type="checkbox"/> Guilty <input type="checkbox"/> Not Gilty	<input type="checkbox"/> Prosecute <input type="checkbox"/> Declined					
2							<input type="checkbox"/> Guilty <input type="checkbox"/> Not Gilty	<input type="checkbox"/> Prosecute <input type="checkbox"/> Declined					
3							<input type="checkbox"/> Guilty <input type="checkbox"/> Not Gilty	<input type="checkbox"/> Prosecute <input type="checkbox"/> Declined					
4							<input type="checkbox"/> Guilty <input type="checkbox"/> Not Gilty	<input type="checkbox"/> Prosecute <input type="checkbox"/> Declined					
5							<input type="checkbox"/> Guilty <input type="checkbox"/> Not Gilty	<input type="checkbox"/> Prosecute <input type="checkbox"/> Declined					

TO: STATE BUREAU OF CRIMINAL IDENTIFICATION • 300 STATE OFFICE BLDG. • SALT LAKE CITY, UTAH 84114

APPENDIX D

SAMPLE USER AGREEMENTS

UTAH CRIMINAL JUSTICE INFORMATION SYSTEM'S
USERS SECURITY AND PRIVACY AGREEMENT

A. GENERAL PROVISIONS

1. Parties. This agreement is made and entered into this _____ day of _____, 19____, by and between the Utah Department of Public Safety, administrator of the Utah Criminal Justice Information System, hereinafter referred to as "System," and _____, hereinafter referred to as "User Agency or Individual."

2. Purpose of Agreement. This agreement provides for System to serve as the state agency responsible for the dissemination of complete and accurate criminal history record information and other criminal justice information between System and User Agency or Individual authorized by federal regulations (28 C.F.R. §20.21). In addition, it provides for security and privacy of information in that dissemination to criminal justice agencies shall be limited to purposes of the administration of criminal justice and criminal justice agency employment, and dissemination to other individuals and agencies shall be limited to those individuals and agencies authorized by federal regulations and shall be limited to the purpose(s) for which it was given and may not be disseminated further.

3. Governing Law. This agreement shall be governed by and interpreted under the laws of the State of Utah.

B. INFORMATION SYSTEM SERVICES

1. Information. In accordance with federal and state regulations, System agrees to furnish User Agency or Individual such complete and accurate criminal history record information and other criminal justice information as is available in the System files and further agrees to furnish such criminal history information and other data as is available through the FBI/NCIC CCH program.

2. Hours. System agrees that User Agency or Individual may use terminal stations at its dispatch center on a 24-hour, seven-day week basis and terminal stations shall provide sufficient authorized personnel to operate them.

3. Liability. It is understood by and between the parties hereto that this agreement shall be deemed executory to the extent of the monies available to System and no liability on account thereof shall be incurred by System beyond monies available to System and no liability on account thereof shall be incurred by System beyond monies available for the purposes thereof.

4. Adjacent Jurisdictions. In keeping with the concept of System as being established to provide assistance to all law enforcement agencies of the state, the User Agency or Individual agrees to serve adjacent criminal justice jurisdictions not equipped with a System terminal, as well as authorized criminal justice employees in transit.

C. SECURITY AND PRIVACY

1. Basis of Eligibility. User Agency or Individual agrees that it is eligible to receive criminal history record information in accordance with federal regulations concerning limitations on dissemination in that User Agency or Individual is either: a criminal justice agency; a non-criminal justice agency or individual acting pursuant to an agreement with a criminal justice agency for the purpose of research; an agency of state or federal government authorized by statute or executive order to conduct employment investigations; or an agency or individual authorized by court order or court rule. Specifically, User Agency or Individual is eligible to receive criminal history record information as _____

2. Limitations on Dissemination. User Agency or Individual agrees to limit dissemination of criminal history record information furnished by System to its own employees and other criminal justice agencies for purposes of the administration of criminal justice and criminal justice agency employment only. In the case of other agencies or individuals, User Agency or Individual agrees that information may be disseminated only to those which qualify under federal regulations and such information shall be limited to the purposes for which it was given and may not be disseminated further. User Agency or Individual agrees that the limited purpose for which the released records may be used is _____

3. Federal and State Regulations. User Agency or Individual further agrees to comply with all federal and state laws, rules, regulations, procedures and policies formally adopted by the Disseminating Agency and the Utah Criminal Justice Information System, and in regard to criminal history record information furnished through the FBI/NCIC CCH program, to rules, procedures, and policies approved by the NCIC Advisory Policy Board and adopted by the NCIC. User Agency or Individual agrees to be bound by the terms of the regulations on a continuing basis with respect to any criminal history record information received from any agency within or outside of the state. Furthermore, the User Agency or Individual subject to these regulations has the burden of giving notice of the requirements of the regulations to other receiving agencies or individuals.

4. Confirming Existence of Record. User Agency or Individual agrees not to confirm the existence or non-existence of criminal history record information for employment or licensing checks, or for any reason whatsoever.

5. Return of Material. User Agency or Individual agrees that all disseminated information and copies thereof shall be retained within its own files and destroyed once the information is no longer needed for the purposes for which it was disseminated. Such information shall be returned to the Disseminating Agency only if such information is an original copy.

6. Contemporary Status of an Individual. Nothing in this agreement or in the 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. 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 disclosed is based on data excluded by the regulations such as wanted posters, court records, or records of traffic offenses.

D. SANCTIONS

1. Cancellation. This agreement may be terminated upon 30 days' written notice by either party hereto and the Disseminating Agency reserves the right to immediately suspend

furnishing any information provided for in this agreement to User Agency or Individual when any rule, policy or procedure adopted by the Disseminating Agency or the Utah Criminal Justice Information System, or approved by the NCIC Advisory Policy Board and adopted by NCIC, or any law of this state or the Federal government applicable to the security and privacy of information is violated or appears to be violated. The Disseminating Agency may reinstate the furnishing of such information upon receipt of satisfactory assurances that such violation did not occur or was corrected. User Agency or Individual also agrees to be subject to a misdemeanor and/or a fine for knowingly violating this agreement or the regulations.

2. Indemnification. The User Agency or Individual hereby agrees to indemnify and save harmless the State of Utah, the Utah Criminal Justice Information System, the Disseminating Agency, and officers, agents, and employees from and against any and all loss, damages, injury, liability, suits and proceedings, however caused, arising directly or indirectly out of any action or conduct of the User Agency or Individual in the exercise or enjoyment of this agreement.

CRIMINAL JUSTICE DISSEMINATING AGENCY

BY _____

TITLE _____

DATE _____

USER AGENCY OR INDIVIDUAL

BY _____

TITLE _____

DATE _____

CRIMINAL JUSTICE DISSEMINATING AGENCY'S
USERS SECURITY AND PRIVACY AGREEMENT

A. GENERAL PROVISIONS

1. Parties. This agreement is made and entered into this _____ day of _____, 19____, by and between

a criminal justice agency operating under the authority of the Utah Department of Public Safety, administrator of the Utah Criminal Justice Information System, hereinafter referred to as "Disseminating Agency," and _____, hereinafter referred to as "User Agency or Individual."

2. Purpose of Agreement. This agreement provides for the Disseminating Agency, under authority of the Utah Criminal Justice Information System, to serve as a state agency responsible for the dissemination of complete and accurate criminal history record information and other criminal justice information between the Disseminating Agency and User Agency or Individual authorized by federal regulations (28 C.F.R. §20.21). In addition, it provides for security and privacy of information in that dissemination to other criminal justice agencies shall be limited to purposes of the administration of criminal justice and criminal justice agency employment, and dissemination to other individuals and agencies shall be limited to those individuals and agencies authorized by federal regulations and shall be limited to the purpose(s) for which it was given and may not be disseminated further.

3. Governing Law. This agreement shall be governed by and interpreted under the laws of the State of Utah.

B. DISSEMINATING AGENCY SERVICES

1. Information. In accordance with federal and state regulations, the Disseminating Agency agrees to furnish User Agency or Individual such complete and accurate criminal history record information and other criminal justice information as is available in the Disseminating Agency's files and further agrees to furnish such criminal history information and other data as is available through the FBI/NCIC CCH program.

2. Hours. The Disseminating Agency agrees that User Agency or Individual may use terminal stations at its dispatch center on a 24-hour, seven-day week basis and terminal stations shall provide sufficient authorized personnel to operate them.

3. Liability. It is understood by and between the parties hereto that this agreement shall be deemed executory to the extent of the monies available to the Disseminating Agency and no liability on account thereof shall be incurred by the Disseminating Agency beyond monies available to the Disseminating Agency and no liability on account thereof shall be incurred by the Disseminating Agency beyond monies available for the purposes thereof.

C. SECURITY AND PRIVACY

1. Basis of Eligibility. User Agency or Individual agrees that it is eligible to receive criminal history record information in accordance with federal regulations concerning limitations on dissemination in that User Agency or Individual is either: a criminal justice agency; a non-criminal justice agency or individual acting pursuant to an agreement with a criminal justice agency for the purpose of research, an agency of state or federal government authorized by statute or executive order to conduct employment investigations; or an agency or individual authorized by court order or court rule. Specifically, User Agency or Individual is eligible to receive criminal history record information as _____

2. Limitations on Dissemination. User Agency or Individual agrees to limit dissemination of criminal history record information furnished by the Disseminating Agency to its own employees and other criminal justice agencies for purposes of the administration of criminal justice and criminal justice agency employment only. In the case of other agencies or individuals, User Agency or Individual agrees that information may be disseminated only to those which qualify under federal regulations and such information shall be limited to the purposes for which it was given and may not be disseminated further. User Agency or Individual agrees that the limited purpose for which the released records may be used is _____

3. Federal and State Regulations. User Agency or Individual further agrees to comply with all federal and state laws, rules, regulations, procedures and policies formally adopted by System and in regard to criminal history record information furnished through the FBI/NCIC CCH program, to rules, procedures, and policies approved by the NCIC Advisory Policy Board and adopted by the NCIC. User Agency or Individual agrees to be bound by the terms of the regulations on a continuing basis with respect to any criminal history record information received from any agency within or outside of the state. Furthermore, the User Agency or Individual subject to these regulations has the burden of giving notice of the requirements of the regulations to other receiving agencies or individuals.

4. Confirming Existence of Record. User Agency or Individual agrees not to confirm the existence or non-existence of criminal history record information for employment or licensing checks, except as provided in the federal regulations for purposes of criminal justice agency employment, statutory authorization expressly referring to criminal conduct, or state and federal investigations determining employment suitability or eligibility for security clearances to classified information.

5. Return of Material. User Agency or Individual agrees that all disseminated information and copies thereof shall be retained within its own files and destroyed once the information is no longer needed for the purposes for which it was disseminated. Such information shall be returned to System only if such information is an original copy.

6. Contemporary Status of an Individual. Nothing in this agreement or in the 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. 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 disclosed is based on data excluded by the regulations such as wanted posters, court records, or records of traffic offenses.

D. SANCTIONS

1. Cancellation. This agreement may be terminated upon 30 days' written notice by either party hereto and System reserves the right to immediately suspend furnishing any information provided for in this agreement to User Agency or Individual when any rule, policy or procedure adopted by System or approved by the NCIC Advisory Policy Board and adopted by NCIC, or any law of this state or the Federal government applicable to the security and privacy of information is violated or appears to be violated. System may reinstate the furnishing of such information upon receipt of satisfactory assurances that such violation did not occur or was corrected. User Agency or Individual also agrees to be subject to a misdemeanor and/or a fine for knowingly violating this agreement or the regulations.

2. Indemnification. The User Agency or Individual hereby agrees to indemnify and save harmless the State of Utah, the System, and the System's officers, agents and employees from and against any and all loss, damages, injury, liability, suits and proceedings howsoever caused, arising directly or indirectly out of any action or conduct of the User Agency or Individual in the exercise or enjoyment of this agreement.

UTAH DEPARTMENT OF PUBLIC SAFETY CONTROL TERMINAL AGENCY

BY _____

TITLE _____

DATE _____

USER AGENCY OR INDIVIDUAL

BY _____

TITLE _____

DATE _____

APPENDIX E

JUVENILE RECORDS DISSEMINATION EXCEPTIONS

This appendix describes the instances where juvenile records can be disseminated without a written release from or on behalf of the juvenile involved.

- (a) The County Attorney
Circumstances: When involved in an investigation of a case which may result in a petition being filed.
Limitation: Court records only except the computer summary.
- (b) Defense Attorney
Circumstances: When defending a juvenile or adult in relation to a petition filed with the Court.
Limitation: Court records only excluding the computer summary and judge's handwritten minutes.
- (c) Division of Family Services
Circumstances: When they have been awarded guardianship or custody or when they are investigating a formal referral made to them regarding dependency, abuse or neglect (55-10-104).
Limitations: None
- (d) Licensed Child Placing Agencies
Circumstances: When they are awarded guardianship, custody or supervisory responsibility by the Court (55-10-104).
Limitations: None
- (e) Schools
Circumstances: Never
Limitations: No records are to be released.
- (f) Youth Services and Other Community Accepted Diversion Agencies
Circumstances: When a youth is referred to them for possible diversion.
Limitations: Diversion agencies shall be told only whether a youth qualifies for diversion or not based on the following criteria. The juvenile is not known to the Court; or less than four (4) status and/or minor offenses; is not on probation; has not been referred to the Court in the past six (6) months and has no pending Court action. Details of the juvenile's record, or the specific reason for inclusion or exclusion should not be discussed or released.
- (g) Law Enforcement Agencies
Circumstances: When investigating an alleged law violation, serving summons, executing a pickup order or bench warrant or determining disposition on a specific referral they have made.
Limitations: Police reports, specific dispositions and identification information only. Complete record summaries, court or probation department records are not to be released.
- (h) Adult Probation and Parole - Division of Corrections
Circumstances: When preparing presentence reports as assigned by Adult Courts or for persons on probation or parole being served by them.
Limitations: None
- (i) Military Authorities
Circumstances: In process of investigation resulting from a person's attempt to join the military.
Limitations: A written record request must be accompanied by a release of information signed by the juvenile, parent or guardian. The Court clerk or her appointed deputy shall

enter a written "yes" if the person has an adjudicated delinquent record and a "no" if no record exists or if the record was closed without a petition, was traffic, dependency or neglect or found not true in court. Details of the juvenile's record or the specific reason for responding yes or no should not be released.

(j) Utah State Industrial School, State Hospital, State Training School

Circumstances: Youth is committed to the above-named institutions (55-10-104).

Limitations: None

(k) Pre-institutional Facilities (Group Homes, Boys' Ranches)

Circumstances: Youth is placed in pre-institutional facility (55-10-104).

Limitations: None

(l) Detention Centers

Circumstances: Custody is being accepted from person or officer who originally took youth in custody or Youth Services Diversion Agency calls and asks for status as described in "f" above.

Limitations: Record Summaries to be shared with authorized officers of the Court only and with Youth Diversion Agencies as prescribed in "f" above.

(m) Juvenile, Parents or Legal Guardian

Circumstances: Petition has been filed and proceedings commenced or summary requested.

Limitations: Court record only except judge's handwritten minutes. Probation Department records only by special order of the Court. If upon review the parent, guardian or juvenile request a record correction, the clerk of the Court shall review the request and authorize the adjustment if justified. Disputes shall be resolved by the judge.

(n) Mental Health

Circumstances: When the Court or probation department orders or requests a review and recommendation from Mental Health.

Limitations: None

(o) Research

Circumstances: (1) Persons or agencies, or any member of the Court staff, desiring to conduct research which in any manner involves the records of the Court, the Court staff, the procedure of the Court, or juveniles who have been found to come within the provisions of section 55-10-77, Utah Code Annotated, 1953, must submit a written request together with full details of the intended research to the Administrative Office of the Juvenile Court for approval. (2) When the intended research involves only the use of court records, court staff, or the procedures of the court, and does not involve the use of any information which may compromise the privacy of juveniles, permission to conduct the research may be granted directly, by the State Administrator of the Juvenile Court, after consultation with the Director of Court Services for the judicial

district involved in the research. (3) When the intended research involves the use of information which may compromise the privacy of juveniles, or when the research requires testing, interviewing, or other communication with the juveniles or their families, the State Administrator may grant permission to conduct the research only with permission of the Judge(s) and the Director of Court Services for the judicial district involved in the research.

Limitations: (1) No juvenile court records or documents may be removed from the Court by any researcher, except records generated by PROFILE, in which any information identifying juveniles has been deleted. (2) If the researching person or agency intends to modify the scope, intent, or procedure of a previously approved research project, written notice including full details of the intended modification must be filed with the Administrative Office of the Juvenile Court. Such modifications will be subject to approval in the same way as the original research request. (3) Upon completion of the research, the researching person or agency will forward to the Administrative Office of the Juvenile Court copies of all reports, summaries, tables, articles, or books produced as a result of the research. Records generated by PROFILE for use in the research must also be returned. (4) Electro-data processing tapes shall be considered records of the Court and shall be subject to the rules previously set forth in this order regarding records, except that tapes may be loaned to persons or agencies after approval by the Administrator of the Juvenile Court and after approval by the Board of Judges of the State of Utah Juvenile Court. Copying, duplicating or otherwise generating additional tapes is forbidden in all instances. (5) At any time, upon the demand of the Administrative Office, all records and information taken from the Court will be returned by the researcher to the Administrative Office. (6) The State Administrator of the Juvenile Court may direct a member of the staff of the Juvenile Court to act as his agent in matters of research, delegating to him all or any of the duties and responsibilities assigned to the Court Administrator as set forth in this order. (7) Exceptions to the provisions of this order may be granted only with the approval of the Board of Juvenile Court Judges.

(p) News Media

The Board of Judges recognizes the public's rights to know concerning the social problems of delinquency and crime and the responsibility of news media to inform the public. We believe that sufficient information should be available so that the public can be aware of the efforts expended and the accomplishments and deficiencies in the correction and rehabilitation of the juvenile offenders. We realize that inadequate information to the public about the work of the Court may undermine confidence in the Court.

1. News Prior to Court Referral: The provisions of the Juvenile Court Code concerning information and records on court cases do not apply to pre-court action in juvenile cases.

News media are not legally restrained from reporting information concerning juvenile offenders that may come from law enforcement sources including the identity of alleged offenders. We urge full reporting of such matters deemed news worthy by news media in the interest of public understanding of the social problems involved.

2. News Representatives Welcome to Information Available in Court: Representatives of public news media are welcome to attend hearings in the Juvenile Court and to report their impressions of the hearings, the facts of the offenses and the details of the court orders in the case. Many cases before the Court involving minor offenses or delinquent behavior not involving the commission of criminal type acts, may not be news worthy except as they may show the procedures and work of the Court and the efforts at correction of the juveniles involved. The identity of children in such cases need not be reported. In cases of wide public interest involving serious vandalism, aggravated public disturbances, repeated disregard for property, repeated theft or felony-type offenses, the Court may release the identity of the juveniles involved for publication.

News media representatives are invited to inquire on the status of individual cases, either to learn the disposition of the Court or to ascertain the stage of the proceedings in a particular case. Upon request in particular types of cases, the Clerk of the Court will notify news media of the hearing so that a reporter may have an opportunity to attend and report on the case.

3. The Juvenile Court will Provide Information: Periodic reports will be released to the Public Information Services. These will include statistical summaries, Court interpretations of actions taken, efforts made to evaluate and improve methods, explanations of rehabilitation programs operating within the Court, general suggestions to parents and juveniles on observations made about the needs in homes and possible constructive programs to be followed, analyses of activities, attitudes, and practices which tend to produce danger and are therefore to be avoided by children and parents.
4. Release of Follow-up Information on Cases Which have Received Public Attention: The Court will release to the Public Information Services reports on the Court dispositions and orders on cases which at the time of their original discovery received widespread attention through the press, radio, and television. These follow-up reports will attempt to give citizens an opportunity to be relieved of the mystery of what happens after the final statement of such original reports "the juveniles were referred to the Juvenile Court."

5. Release of Information to Private Persons Who Are Victims of Juvenile Vandalism or Other Offenses: Persons damaged as a result of delinquent acts for which juveniles are referred to Juvenile Court may attend the hearing on the matter and at their request, the Clerk will notify them of the hearing. If they cannot or do not wish to attend, they will be advised of the Court's disposition upon request.

APPENDIX F

AGENCIES AUTHORIZED ACCESS

TO CRIMINAL HISTORY RECORD INFORMATION

TYPE OF AGENCYAGENCY AUTHORIZEDAUTHORIZATIONState Criminal
Justice Agencies

Adult Probation and Parole	U.C.A.	§ 77-62-35
Utah State Prison	U.C.A.	§ 64-9-28
Division of Corrections	U.C.A.	§ 77-62-30
Sheriff and Police Officers	U.C.A.	§ 77-59-18(1)
Other State and federal Criminal Identification Bureaus	U.C.A.	§ 77-59-18(2) (21)
Public Officers	U.C.A.	§ 77-59-22
Prosecuting Attorneys	U.C.A.	§ 77-59-18(3)
Judges	U.C.A.	§ 77-59-18(4)
Highway Patrol	U.C.A.	§ 27-10-5,6
Peace Officers	U.C.A.	§ 77-59-25
State Fire Marshall	U.C.A.	§ 63-29-22 § 77-10-6
Department of Public Safety	U.C.A.	§ 77-59-1 et seq.
Wildlife Resources	U.C.A.	§ 23-10-1

State
Non-Criminal
Justice Agencies

Insurance Department	U.C.A.	§ 31-17-50 § 31-2-3(4)
Industrial Commission	U.C.A.	§ 35-1-19,31,88
Utah Bar Association	U.C.A.	§ 78-51-1,10,12
Liquor Commission	U.C.A.	§ 32-4-14
Motor Vehicle Division	U.C.A.	§ 41-3-26
Medical Association	U.C.A.	§§ 58-12-31(8),25,35,36
Pharmaceutical Ass'n.	U.C.A.	§§ 58-17-2,3

Non-State
Non-Criminal
Justice Agencies

BankAmericard	U.C.A.	§ 77-59-27
Master Charge	U.C.A.	§ 77-59-27

APPENDIX G

COMPUTER SECURITY GUIDELINES
FOR IMPLEMENTING
THE PRIVACY ACT OF 1974

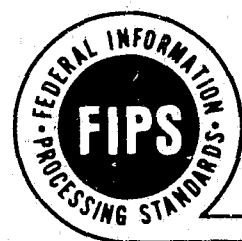


FIPS PUB 41

**FEDERAL INFORMATION
PROCESSING STANDARDS PUBLICATION**

1975 MAY 30

U.S. DEPARTMENT OF COMMERCE / National Bureau of Standards



COMPUTER SECURITY GUIDELINES FOR IMPLEMENTING THE PRIVACY ACT OF 1974

CATEGORY: ADP OPERATIONS

SUBCATEGORY: COMPUTER SECURITY

Foreword

The Federal Information Processing Standards Publication Series of the National Bureau of Standards is the official publication relating to standards adopted and promulgated under the provisions of Public Law 89-306 (Brooks Bill) and under Part 6 of Title 15, Code of Federal Regulations. These legislative and executive mandates have given the Secretary of Commerce important responsibilities for improving the utilization and management of computers and automatic data processing systems in the Federal Government. To carry out the Secretary's responsibilities, the NBS, through its Institute for Computer Sciences and Technology, provides leadership, technical guidance, and coordination of government efforts in the development of technical guidelines and standards in these areas.

The selective application of technological and related procedural safeguards is an important component of the Federal Government's efforts to protect the privacy of individuals, as required by the Privacy Act of 1974. The guidelines provided by this publication establish the groundwork for assessing the risks of unauthorized disclosures of personal data in current automated systems and developing a set of safeguards to minimize those risks. They are made available for use by Federal agencies within the context of the Office of Management and Budget's total program for implementing the Privacy Act.

RUTH M. DAVIS, Director
Institute for Computer Sciences
and Technology

Abstract

This publication provides guidelines for use by Federal ADP organizations in implementing the computer security safeguards necessary for compliance with Public Law 93-579, the Privacy Act of 1974. A wide variety of technical and related procedural safeguards are described. These fall into three broad categories: Physical security, information management practices, and computer system/network security controls. As each organization processing personal data has unique characteristics, specific organizations should draw upon the material provided in order to select a well-balanced combination of safeguards which meets their particular requirements.

Key words: Access controls; ADP security; computer security; Federal Information Processing Standards; information management; personal data; physical security; privacy risk assessment.

Nat. Bur. Stand. (U.S.), Fed. Info. Process. Stand. Publ. (FIPS PUB) 41, 20 pages, (1975) CODEN: FIPPAT

For sale by the Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402. (Order by SD Catalog No. C13.52:41). GPO price 70 cents.



Federal Information Processing Standards Publication 41

1975 May 30



ANNOUNCING THE

COMPUTER SECURITY GUIDELINES FOR IMPLEMENTING THE PRIVACY ACT OF 1974

Federal Information Processing Standards Publications are issued by the National Bureau of Standards pursuant to the Federal Property and Administrative Services Act of 1949 as amended, Public Law 89-306 (79 Stat. 1127), and as implemented by Executive Order 11717 (38 FR 12315, dated May 11, 1973), and Part 6 of Title 15 CFR (Code of Federal Regulations).

Name of Guideline: Computer Security Guidelines for Implementing the Privacy Act of 1974.

Category of Guideline: ADP Operations, Computer Security.

Explanation: The Privacy Act of 1974 imposes numerous requirements upon Federal agencies, to prevent the misuse or compromise of data concerning individuals. Federal ADP organizations which process personal data must provide a reasonable degree of protection against unauthorized disclosure, destruction or modification of personal data, whether intentionally caused or resulting from accident or carelessness. These guidelines provide a handbook for use by Federal organizations in implementing any computer security safeguards which they must adopt in order to implement the Act. They describe risks and risk assessment, physical security measures, appropriate information management practices, and computer system/network security controls.

Approving Authority. Department of Commerce, National Bureau of Standards (Institute for Computer Sciences and Technology).

Maintenance Agency. Department of Commerce, National Bureau of Standards (Institute of Computer Sciences and Technology).

Cross Index. See Appendix.

Applicability. These guidelines were prepared at the specific request of the Office of Management and Budget and are intended for use in implementing the computer security requirements imposed by the Privacy Act of 1974. As they treat the general problem of computer security in addressing a host of available safeguards, they are also generally applicable to computer security matters unrelated to individual privacy.

Implementation. Each Federal ADP organization has unique requirements for computer security stemming from the Privacy Act of 1974. Specific needs depend on the organization's personal data processing mission and its operating environment. Utilizing the description of a wide variety of safeguards contained in these guidelines, an organization may select a well-balanced set which meets its particular needs.

Specifications. Federal Information Processing Standard 41 (FIPS 41), Computer Security Guidelines for Implementing the Privacy Act of 1974, (affixed).

Qualifications. This document provides a set of guidelines from which a Federal organization may select technical and related procedural safeguards for protecting personal data in automated information systems. It does not cover topics such as determination of the need for maintaining personal data and the relevance of the data to the performance of authorized functions. Also, matters such as employee rules of conduct, employee screening and training are outside the purview of this document.

As each organization has a unique set of requirements and risks to consider, depending on its environment, function and operations, no list of required safeguards can be prescribed in general. Each organization must analyze its own requirements. Computer security is only one facet of implementation of the Privacy Act of 1974, and this document therefore should be considered in conjunction with other issuances of the Office of Management and Budget, the General Services Administration, and the Civil Service Commission.

As new knowledge, techniques and devices become available in the future, these guidelines will need to be modified accordingly. Because of the new requirements of the Privacy Act of 1974 and anticipated technical and related procedural experiences, much information relevant to these guidelines will be gained. All comments and critiques are welcome, and will be considered in future revision. They should be addressed to the Systems and Software Division, Institute for Computer Sciences and Technology, National Bureau of Standards, Washington, D.C. 20234.

Where to Obtain Copies of the Standard.

a. Copies of this publication are available from the Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402 (SD Catalog Number C13.52:41). There is a 25 percent discount on quantities of 100 or more. When ordering, specify document number, title, and SD Catalog Number. Payment may be made by check, money order, coupons, or deposit account.

b. Microfiche of this publication is available from the National Technical Information Service, U.S. Department of Commerce, Springfield, Virginia 22151. When ordering refer to Report Number NBS-FIPS-PUB-41 and title. Payment may be made by check, money order, or deposit account.

Executive Overview

The Privacy Act of 1974 (5 U.S.C. 552a) imposes numerous requirements upon Federal agencies to prevent the misuse of information about individuals and assure its integrity and security. These requirements will be met by the application of selected managerial, administrative and technical procedures which, in combination, can be used to achieve the objectives of the Act.

This document provides a set of guidelines for the use of technical procedures for safeguarding personal data in automated information systems. Managerial and administrative procedures such as those relating to basic determinations concerning the need for maintaining personal data and its relevance to the performance of authorized functions, employee rules of conduct, and employee screening and training are outside the purview of this document. The guidelines were prepared in response to the Office of Management and Budget memorandum dated March 12, 1975, *Implementation of the Privacy Act of 1974*, and are made available for consideration and use by all Federal agencies in meeting the requirements of the Act. They represent, however, only one segment of the Government-wide guidance that is provided for in OMB's circular governing the implementation of the Act and should, therefore, be considered in conjunction with all other guidance on this subject.

There are three categories of technical safeguards which can be used to maintain the integrity of personal information and protect it from unauthorized use. These categories are: physical security procedures, information management practices and computer system/network security controls. The guidelines cover all three categories; neither category by itself is likely to offer protection against all risks of privacy violations. However, by carefully selecting appropriate components from among all three categories and packaging them into a well-balanced set of safeguards according to individual needs, the level of protection can usually be improved significantly at reasonable cost.

The relevance and utility of these technical procedures can be grasped quickly if they are viewed in the context of the Privacy Act of 1974. Figure 1, on page 2, identifies the principal provisions of the Act which involve the application of safeguards and shows how each of the three categories can contribute to the implementation of these provisions. The matrix illustrates graphically not only that the procedures can be used in combination to administer various provisions of the Act, but also that some safeguards can simultaneously contribute to satisfying more than one provision. Significantly, it also indicates that the preservation of data integrity and security in automated systems can be achieved in good measure by the prudent use of physical security and information management practices and is not necessarily dependent upon complex computer system/network controls.

The major provisions of the Privacy Act which most directly involve the use of computer system/network controls are: Subsection (b) of 5 U.S.C. Section 552a which limits the disclosure of personal information to authorized persons and agencies; Subsection (e) (5) which requires the maintenance of accurate, relevant, timely, and complete records; and Subsection (e) (10) which requires the use of safeguards to insure the security and integrity of records. Although the Act sets up legislative prohibitions against unauthorized disclosures, system/network controls are also needed to help assure that access to personal data is properly controlled and that intentional or accidental violations of security and integrity do not occur.

These controls include techniques for providing positive identification of the authorized user of the system and remote terminals, authenticating his right to have access to specific data in a system shared by others and preventing him from gaining access to data and/or programs to which he is not entitled, and, finally, providing a system of internal audits for monitoring compliance with the stipulated security requirements. In cases involving the automated transfer of personal data between terminals and a computer system or among systems, protection requirements might, on infrequent occasions, be judged sufficiently strong to warrant the use of data encryption techniques.

Thus, in addition to viewing the technological safeguards in terms of the provisions of the Privacy Act, it is useful also to view them in terms of the control points within a computer system/network where security risks occur and where appropriate safeguards can be applied. This perspective is provided in figure 2 on pages 4 & 5, which portrays the elements of a computer system/network, beginning with the off-line storage of data in machine-readable media (e.g., tapes and discs) and progressing through the many possible processing modes, including the use of interactive computer terminals at local and remote locations and the linking of local systems via communications networks. It stresses again the value of physical security and information management practices as major adjuncts to the computer system/network security controls of the type described in the preceding paragraph.

In order to provide for consistency and effectiveness in applying protective measures, the National Bureau of Standards has identified the need for technical standards and guidelines in the following topical areas:

- Physical security
 - Risk management
 - Fire and other disasters
 - Physical protection
 - Contingency planning
- Information management
 - Data input, storage and handling
 - Record identification
 - Media control
 - Programming techniques for security
 - Software documentation
 - Data elements
- Computer system/network security controls
 - User identification
 - Terminal identification
 - Data access controls
 - Data encryption
 - Security auditing

Within these topical areas, the National Bureau of Standards has already provided the following guidelines which are available and can be obtained as indicated in the Appendix:

- Executive Guide to Computer Security
- Guidelines for ADP Physical Security and Risk Management

It is intended that the standards and guidelines identified above will be examined, developed and published using regular or expedited procedures that are consistent with meeting the needs and problems generated by experience gained in administering the Privacy Act. Meanwhile, the guidelines included in this document are intended as a statement of technical measures which managers should consider together with managerial and administrative procedures as they decide upon a balanced set of safeguards suitable to their specific operational needs and environments.

Inquiries and comments regarding the application of these guidelines should be directed to the Systems and Software Division, Institute for Computer Sciences and Technology, National Bureau of Standards, Washington, D.C. 20234. (Telephone: Area Code 301-921-3861)



Federal Information Processing Standards Publication 41

1975 May 30

Specifications for



COMPUTER SECURITY GUIDELINES FOR IMPLEMENTING THE PRIVACY ACT OF 1974

Contents

	Page
Executive Overview	3
1. INTRODUCTION	7
1.1. The Privacy Act of 1974	7
1.2. Scope of Guidelines	7
1.3. Definitions	7
1.4. Safeguards	7
2. SECURITY RISK ASSESSMENT AND SAFEGUARD SELECTION	9
2.1. Security Risk Assessment	9
2.2. Categories of Security Risks	12
2.2.1. Accidents, Errors, and Omissions	12
2.2.2. Risks from Uncontrolled System Access	12
2.2.3. Risks from Authorized Users of Personal Data	13
2.2.4. Risks from the Physical Environment and from Malicious Destructive Acts	13
2.2.5. Risks from Deliberate Penetrations	13
2.3. Cost Considerations for Selecting Safeguards	13
3. PHYSICAL SECURITY	14
3.1. Entry Controls	15
3.2. Storage Protection	15
4. INFORMATION MANAGEMENT PRACTICES	15
4.1. Handling of Personal Data	16
4.2. Maintenance of Records to Trace the Disposition of Personal Data	16
4.3. Data Processing Practices	16
4.4. Programming Practices	17
4.5. Assignment of Responsibilities	17
4.6. Procedural Auditing	17
5. SYSTEMS SECURITY	17
5.1. Identification	17
5.2. System Access Controls	18
5.3. Access Auditing	18
5.4. Network Systems	18
5.5. Planning for Future ADP Systems	19
5.5.1. Internal Controls	19
5.5.2. Data Encryption	19

1. Introduction

1.1. The Privacy Act of 1974

The Privacy Act of 1974 imposes numerous requirements upon Federal agencies to prevent the misuse of data about individuals, respect its confidentiality and preserve its integrity. Federal agencies can meet these requirements by the application of selected managerial, administrative and technical procedures which, in combination, achieve the objectives of the Act.

The major provisions of the Privacy Act which most directly involve computer security are found in the following parts of 5 U.S.C. Section 552a:

- Subsection (b), which limits disclosure of personal information to authorized persons and agencies;
- Subsection (e) (5), which requires accuracy, relevance, timeliness and completeness of records;
- Subsection (e) (10), which requires the use of safeguards to insure the confidentiality and security of records.

Although the Act sets up legislative prohibitions against abuses, technical and related procedural safeguards are required in order to establish a reasonable confidence that compliance is indeed achieved. It is thus necessary to provide a reasonable degree of protection against unauthorized disclosure, destruction or modification of personal data, whether intentionally caused or resulting from accident or carelessness.

1.2. Scope of Guidelines

This document was prepared at the request of the Office of Management and Budget. It provides a set of guidelines specifying technical and related procedural methods for protecting personal data in automated information systems and should be read in conjunction with OMB's circular on the implementation of the Privacy Act. Managerial and administrative procedures such as those relating to basic determinations concerning the need for maintaining personal data and its relevance to the performance of authorized functions, employee rules of conduct, and employee screening and training are outside the purview of this document. These guidelines represent only one aspect of Government-wide implementation guidance. Like the National Bureau of Standards, the General Services Administration and the Civil Service Commission have issued guidelines dealing with specific topics, under direction of the Office of Management and Budget.

1.3. Definitions

The following terminology is used throughout this document in discussing the treatment of data:

- Confidentiality—A concept which applies to data. It is the status accorded to data which requires protection from unauthorized disclosure.
- Data Integrity—The state existing when data agrees with the source from which it is derived, and when it has not been either accidentally or maliciously altered, disclosed or destroyed.
- Data Security—The protection of data from accidental or intentional, but unauthorized, modification, destruction or disclosure.

Safeguards which provide data protection are grouped into three categories: physical security measures, information management practices, and computer system/network security controls. Specifically, these are:

- Physical Security Measures—Measures for protecting the physical assets of a system and related facilities against environmental hazards or deliberate actions.
- Information Management Practices—Procedures for collecting, validating, processing, controlling and distributing data.
- Computer System/Network Security Controls—Techniques available in the hardware and software of a computer system or network for controlling the processing of and access to data and other assets.

1.4. Safeguards

The relevance and utility of these technical safeguards can be grasped quickly if they are viewed in the context of the Privacy Act of 1974. Figure 1 identifies the principal provisions of the Privacy Act which involve the application of safeguards and shows how each of the three categories can contribute to the implementation of these provisions. The matrix also serves to illustrate graphically that adopting particular safeguards may help to satisfy more than one requirement of the Act. Significantly, it also indicates that protection of data in automated systems is not necessarily dependent upon complex computer system/network technology, but can be achieved in good measure by the prudent use of physical security measures and information management practices.

The safeguards discussed here are aimed specifically at precluding unauthorized access to personal data in computer systems, but most of

them, especially those in the areas of physical security and information management, are applicable to manual as well as automated systems. Most of them also provide protection for other kinds of data than personal. However, since the present emphasis is on personal data, "data" is synonymous with "personal data" in the remainder of this document.

Figure 1 relates technological safeguards to specific provisions of the Privacy Act. Alternatively, they may be viewed in relation to the control points within a computer system/network where security risks occur and where appropriate safeguards can be applied. This perspective is provided in figure 2 on pages 10 and 11, which shows the elements of a computer network, beginning with the offline storage of data in machine-readable media (e.g., tapes and disks) and progressing through the many possible processing modes, including the use of interactive computer terminals at local and remote locations and the linking of local systems via communications networks. It stresses again the value of physical security measures and information management practices, in relation to computer system/network controls.

These guidelines cover the three categories of safeguards defined in Section 1.2. The consideration of one to the exclusion of the others is not likely to offer protection against all risks of privacy violations. However, by carefully selecting a well-balanced set of safeguards, the level of protection can usually be improved significantly at reasonable cost.

SAFEGUARDS	SECTION OF GUIDELINES	SUBSECTION OF 5 U.S.C. SECTION 552a								
		REQUIREMENTS	(b)	(c) (1)	(d)	(d) (4)	(e) (1)	(e) (5), (6)	(e) (10)	(1) (1)
		Control of Disclosures								
		Accounting of Disclosures								
		Provide Access to Records								
		Inclusion of Disputed Information								
		Use Relevant Data Only for Authorized Purposes								
		Maintain Accurate, Complete Records								
		Insure Integrity, Security and Confidentiality of Records								
		Retention of Records; Archival Storage								
Physical Security	3.0									
Entry Controls	3.1		X						X	
Storage Protection	3.2		X					X	X	X
Information Management Practices	4.0									
Handling of Data	4.1		X		X				X	X
Maintenance of Records	4.2		X	X					X	
Data Processing Practices	4.3		X	X		X	X	X	X	
Programming Practices	4.4		X	X		X	X	X	X	
Assignment of Responsibilities	4.5		X						X	X
Procedural Auditing	4.6		X	X		X		X	X	X
Systems Security	5.0									
Identification	5.1		X		X		X		X	
Access Controls	5.2		X		X		X	X	X	
Access Auditing	5.3		X	X	X		X		X	X
Data Encryption	5.5.2		X				X	X	X	X

FIGURE 1. Technical safeguards applied to requirements of the Privacy Act of 1974.

2. Security Risk Assessment and Safeguard Selection

The most important managerial actions a Federal agency must take initially are first, to make sure that any records which the agency maintains are necessary and relevant to the performance of a lawful agency function and second to restrict authorizations for access to personal data to a minimum. A fundamental principle underlying the Privacy Act is that information not maintained about an individual cannot be misused to his detriment. The elimination of non-essential information not only reduces the likelihood of harmful actions, but, by keeping record-keeping practices to a minimum, also eases the task of safeguarding the essential data.

The technical requirements of the Privacy Act for safeguarding the confidentiality, integrity, and security of personal data are less detailed and specific than some of the other requirements. The level of security needed to support privacy depends on the uses which are made of the records, the uses which others could make of the records if they are inadvertently or intentionally disclosed and the harm that might accrue to the individual. Furthermore, security needs are dependent on the environment in which the system of records operates. The determination of which security safeguards are needed to protect a given system must be made by personnel who are very familiar with the information maintained and with the administrative, technical, and physical environment in which the system operates.

2.1. Security Risk Assessment

The first step toward improving a system's security is to determine its security risks. A security risk assessment benefits an agency in three ways:

- (1) It provides a basis for deciding whether additional security safeguards are needed.
- (2) It ensures that additional security safeguards will help to counter all the serious security risks.
- (3) It saves money that might have been wasted on safeguards which do not significantly lower the overall risks and exposures.

The goal of a risk assessment is to identify and prioritize those events which would compromise the integrity and confidentiality of personal data. The seriousness of a risk depends both on the potential impact of the event and its probability of occurrence.

Section 2.2 identifies certain general risks and discusses general priorities. A risk assessment

can be successful even though it only identifies the most serious risks without attempting to quantify degrees of risk; however, the degree of risk should be estimated in quantitative terms when possible. This provides a better basis for deciding what security safeguards are necessary and reasonable. It is sometimes possible to arrive at quantified estimates of risk which, though inexact, are still adequate for the purpose of selecting appropriate safeguards.

Estimates of the expected frequency of accidental risks can be based on previous experience of the agency and of other agencies with similar record systems. For risks that arise from deliberate acts, estimate the cost of carrying out the threat. Risks of deliberate penetration are far more likely when someone can benefit substantially from the act—especially when the act requires little effort or knowledge on his part. An operator with free access to the agency's ADP center may browse through sensitive files at virtually no cost to himself, whereas an individual intent on the unlikely act of undetectable interception of computer transmissions may require major capital and operating investments.

- In general the risk assessment should consider all risks—not just risks to personal data. While these guidelines emphasize the security of personal data, it is best to develop an integrated set of security safeguards which protect all valuable data on the system wherever possible.

The risk assessment should be conducted by a team which is fully familiar with the problems that occur in the daily handling and processing of the information. The participants on the risk assessment team should include experienced representatives from:

- (1) the operating unit supported by or having jurisdiction over the data under consideration,
- (2) the programmers responsible for support of the operation or function under consideration.
- (3) the unit responsible for managing ADP operations,
- (4) the system programmers—if the agency has this as a separate function,
- (5) the person assigned the responsibility for overseeing or auditing system security.
- (6) those responsible for physical security.

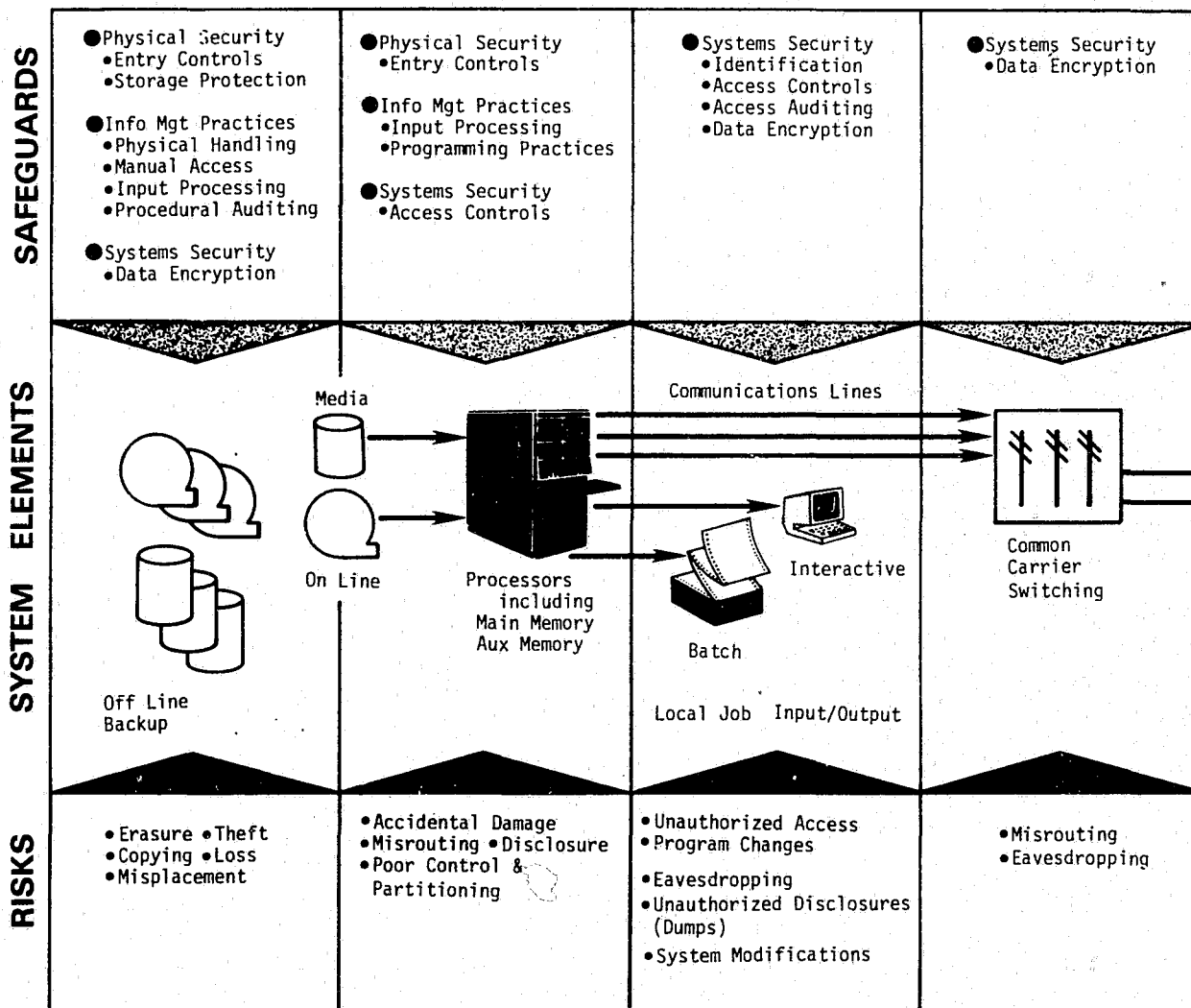
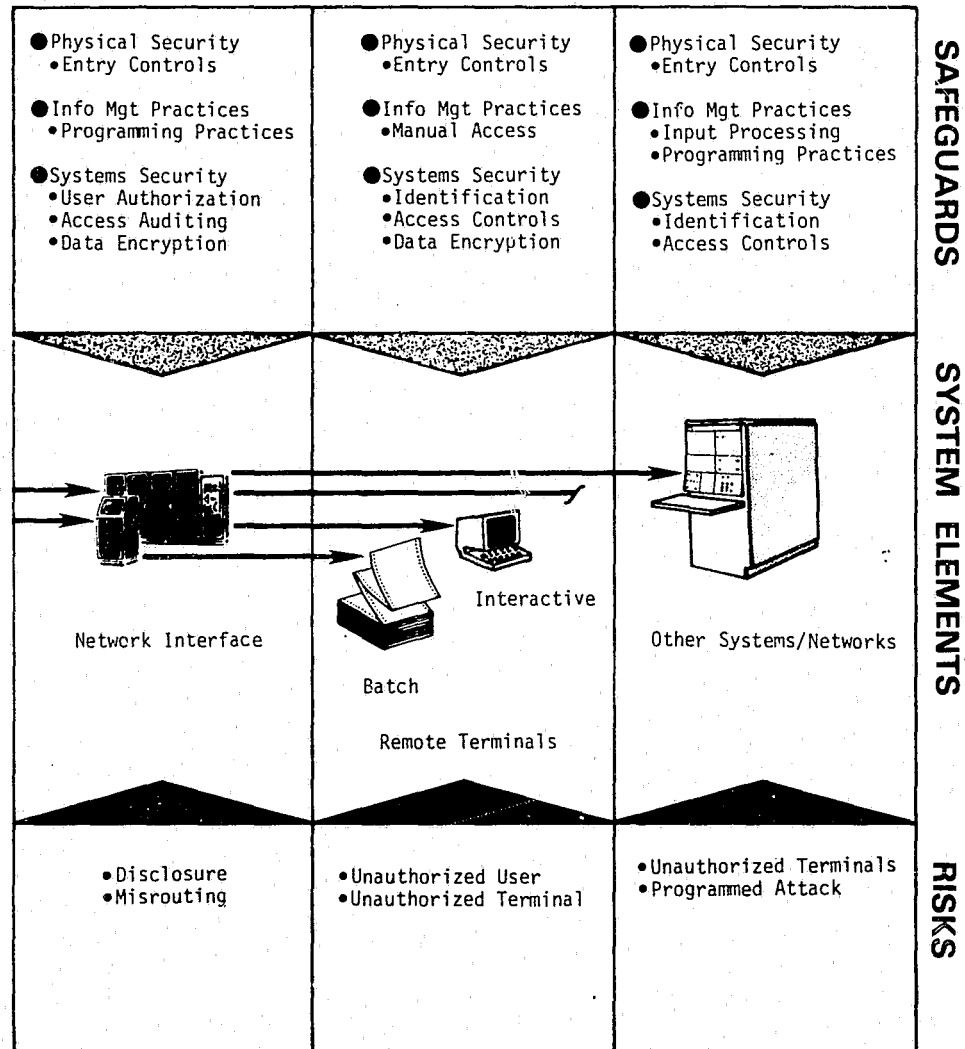


FIGURE 2. Technical safeguards and data security risks.



2.2. Categories of Security Risks

In this section general classes of security risks are identified and categorized as an initial illustration of risk assessment and as a step toward understanding the scope of security concerns. Risks must be assessed with respect to every file of personal information in the system. Each agency will have to identify its specific risks and evaluate the impact of those risks in terms of its information files.

The risks listed in the following subsections progress from acts of carelessness to system penetrations requiring significant technical sophistication. Risks are generally listed in the order in which they are likely to be encountered; however, each agency must realize that its risks could be prioritized differently if unique circumstances exist. Those agencies designing new ADP systems—especially large, remote-access systems—should consider the risks of deliberate system penetration at the time they are initially determining the system configuration.

2.2.1. Accidents, Errors, and Omissions

Experience indicates that the most commonly encountered security risks are usually accidents, errors and omissions. The damage from these accidental events far exceeds the damage from all other security risks. Good information management practices are necessary to reduce the damage that can result from these occurrences.

Some examples of these risks are:

- Input error—Data may not be checked for consistency and reasonableness at the time they are entered into the system; or data may be disclosed, modified, lost, or misidentified during input processing.
- Program errors—Programs can contain many undetected errors—especially when they are written with poor programming practices or are not extensively tested. A program error may result in undesirable modification, disclosure or destruction of sensitive information.
- Mistaken processing of data—Processing requests may update the wrong data; for example, if a tape is mounted at the wrong time.
- Data loss—Data on paper printouts, magnetic tapes, or other removable storage media may be lost, misplaced, or destroyed.

- Improper data dissemination—Disseminated data may be misrouted or mislabeled, or it may contain unexpected personal information.
- Careless disposal—Personal data can be retrieved from waste paper baskets, magnetic tapes, or discarded files.

2.2.2. Risks from Uncontrolled System Access

Agencies expose themselves to unnecessary risks if they fail to establish controls over who can access the personal data which is processed on their ADP systems. Outsiders must not have free access to the personal data. The number of agency employees with access to personal data must also be kept as small as possible without hindering the mission of the agency.

Physical security measures are always needed to control system access. If everyone using the ADP system is authorized access to all the personal data being processed, then physical security measures can adequately control system access. If the system is also used by some who should not be authorized access to all types of personal data, then information handling practices and system access controls are also needed to control these risks.

Examples of these risks include:

- Open system access—There may be no control over who can either use the ADP system or enter the computer room.
- Theft of data—Personal data may be stolen from the computer room or other places where it is stored.
- Unprotected files—Data files may not be protected from unauthorized access by other users of the ADP system. This applies to on-line files and also to off-line files such as magnetic tapes. The latter are sometimes accessible simply by requesting that they be mounted.
- Dial-in access—There is serious danger that unauthorized persons can access the system when remote, dial-in access is allowed.
- Open access during abnormal circumstances—Data which is adequately protected during normal operations may not be adequately protected under abnormal circumstances. Abnormal circumstances, include power failures, bomb threats, and natural disasters such as fire or flood.

2.2.3. Risks from Authorized Users of Personal Data

Experience with computer-related crime indicates that the most serious risks from deliberate acts are from employees who work with the data. These employees often know exactly what security safeguards are in effect, and they may know how to get around them as well. Protection of personal data from abuse by those authorized to access it is an important security concern.

Practices which contribute to these risks include:

- Poorly defined criteria for authorized access—Personnel may not know whether another employee should have access to a data item.
- Lax attitude toward employee dishonesty—Employee dishonesty may be relatively common and tolerated by management. Rules of conduct for agency employees having access to personal data must be established.
- Unaudited access to personal data—If an individual can access personal data knowing that there is no audit trail recording his access, then he will feel he cannot be held accountable for that act.

2.2.4. Risks from the Physical Environment and from Malicious Destructive Acts

Physical destruction or disabling of the ADP system is not usually a primary risk to privacy. Environmental hazards and malicious acts may destroy records required by the Privacy Act, or they may damage the accuracy, timeliness, or completeness of records. However, these risks are also serious because of the value of the resources that might be destroyed and because the agency's mission is often dependent on records in the ADP system. Security safeguards—including file back-up and contingency planning—needed and usually provided for these other reasons will normally be more than adequate to protect privacy against these risks.

Examples of these risks include:

- Fire, heat, water damage, and flood
- Electric power failure
- Malicious destruction by employees or outsiders.

2.2.5. Risks from Deliberate Penetrations

Current computer systems are vulnerable to deliberate penetrations, which can bypass

routine security controls. These penetrations usually require the participation of an individual with specific technical knowledge. To date, there have been relatively few instances of substantial harm resulting from such deliberate penetrations. Thus these risks now appear to be less likely than most of the other risks mentioned above. The knowledgeable penetrator usually acts rationally, and the personal data would have to be very valuable to be attractive to him. However, agencies should be aware that attackers may try to embarrass the agency by demonstrating that their personal data is not secure.

In the future, risks from deliberate penetrations could become more significant. These potential risks will be greatly magnified by large computer networks. Agencies that are designing such networks for future use should consider these risks in the early planning stage.

Deliberate penetration risks include:

- Misidentified access—Passwords are often used to control access to a computer or to data, but they are notoriously easy to obtain if their use is not carefully controlled. Furthermore, a person may use an already logged-in terminal which the authorized user has left unattended, or he may capture a communications port as an authorized user attempts to disconnect from it.
- Operating system flaws—Design and implementation errors in operating systems allow a user to gain control of the system. Once the user is in control, he can disable auditing controls, erase audit trails, and access any information on the system.
- Subverting programs—Programs containing hidden subprograms that disable security protections can be submitted. Other programs can copy personal files into secret or misidentified files to use when protection is relaxed.
- Spoofing—Actions can be taken to mislead system personnel or the system software into performing an operation that appears normal but actually results in unauthorized access.
- Eavesdropping—Communications lines can be "monitored" by unauthorized terminals to obtain or modify information or to gain unauthorized access to an ADP system.

2.3. Cost Considerations for Selecting Safeguards

Each agency should consider the cost of each safeguard when selecting from among the several options available. While each agency must consider its own unique circumstances in assess-

ing costs, general guidelines for understanding cost parameters will assist in developing priorities for action.

Costs fall into two major areas: initial and operating costs. Initial costs include the purchase of new system elements, modification of existing systems to accept the new element, one-time administrative measures to support the new elements, and the initial testing of their effectiveness. Operating costs include the increased day-to-day costs of running the enhanced system, including such cost components as personnel, computer processing, storage, and system monitoring.

Security is needed as a prerequisite to privacy, but it is also needed for many other reasons. Basic security safeguards adequate to protect other valuable data such as financial and payroll records may also be adequate to support privacy. Only a small fraction of overall computer security costs is likely to be attributable to privacy. Agencies should wherever feasible keep the costs of security measures installed for other reasons separate from the costs of assuring privacy.

A risk assessment will have identified those risks which need to be controlled. Sections 3, 4, and 5 discuss various security controls which can be used. When these protection mechanisms are selected they should constitute a system of complementary measures that provide protection where it is needed. Each protective measure should be assessed in terms of the *incremental* protection achieved by the additional cost. A small amount spent for protection may increase the cost of intentional damage beyond an acceptable limit. A lock on a tape cabinet may provide all the protection needed for certain files since the simple lock raises an act of unauthorized access to one of "breaking-in." On the other hand, it would provide little protection against an irrational act of vandalism.

Physical security should be reviewed first, and improved where necessary. For most agencies, the application of physical security measures provides sufficient protection against intentional or overt external acts against agency data. However, it provides little protection against accidental or unintentional damage to files or against overt internal acts. Appropriate *information management practices* will provide a significant level of protection against many risks not covered by physical security. *System security safeguards* should be considered by those agencies whose data sensitivity levels require more protection than that offered by physical security and information management practices.

3. Physical Security

Physical security as it pertains to the protection of data does not differ from physical security for protecting other resources. It is achieved through the use of locks, guards, and administratively controlled procedures as well as measures required for the protection of the structures housing the computer and related equipment against damage from accident, fire and environmental hazard, thus ensuring the protection of their contents. Extensive guidelines for assessing physical security risks and applying appropriate measures are provided in *Guidelines for Automatic Data Processing Physical Security and Risk Management* (see Appendix). This section highlights considerations for determining the need for and application of physical security measures.

Security at an entrance to a computer center can prevent entry by all but the most determined intruders. Prevention of unauthorized entry into a facility can be accomplished not only by establishing a guard force but also by controlling all possible means of access from the exterior, including even such remote avenues as air conditioning vents, and through the use of sign-in procedures, badges for authorized personnel, special locks, exterior lighting, TV cameras, barriers (fences), and intrusion detection devices.

A thorough survey of the environment of a facility will disclose any special dangers in the area such as chemical or explosives activity or likelihood of flood, improper storage of combustibles, inadequate visitor control and other obvious hazards which could result in situations where data might be destroyed or exposed to public scrutiny or haphazard removal. In fact, such obvious perils should be considered before selecting the location for a computer facility although they are sometimes unavoidable.

It is reasonable to assume that protection against fire, explosion and natural disasters will be available in any computer installation, but additional measures may be necessary to insure the confidentiality and security of records. The risks to data which can be generated by a disaster situation stem not only from the vulnerability of the data's storage medium to destruction occurring during the actual catastrophe but extend to subsequent exposure of the media, reports and source materials in a damaged facility. In a disaster, accidental or not, risks to stored data also include damage caused by weather, firefighting techniques, salvage operations, vandalism, or theft.

While no hard and fast rules exist to determine the need or extent of physical protection measures for a given situation, a number of possibilities exist that should be considered. For any specific installation, some set of the measures described below must be selected for implementation in order to provide adequate safeguards against the unauthorized destruction, disclosure or modification of personal data.

3.1. Entry Controls

- Limit the number of entrances to the computer facility to a minimum. (There should be coordination of this measure with those responsible for fire protection and building security.) Doors should be of sufficient strength to resist forced entry.
- Install a screening device at every entrance, be it a guard, a badge reader, an electronic lock, a TV camera manned by a guard in another location, or a physical lock. Maintain entry logs wherever possible. Monitor closely all items moving into or out of the facility, whether expected or not, e.g., a scheduled delivery.
- If there is an extensive perimeter requiring protection, consider use of exterior lighting, TV cameras, roving patrols, intrusion detection devices; however, such protection is usually not the responsibility of the ADP manager.
- Secure all openings through which an intruder could gain entrance or receive material.
- Control the use of badges to permit entry. They should not be issued in such quantity that guards cannot verify badge holders. When people leave the employ of the facility, whatever the reason, it is essential to retrieve all keys, badges, etc., which have been issued to them. Visitors should be issued temporary badges differing in appearance from employee badges.
- In case of any unusual diversions such as power outages, bomb threats, false fire alarms, make a thorough search of the facility to prevent or to uncover loss or destructive activity which might have taken place during any confusion. Entry logs or other records of facility activity should be consulted; they might reveal any unusual occurrence that could serve as a clue to the identity of the perpetrator of the event.
- Provide adequate protection for remote terminals, tape libraries, trash areas, etc., which are not within the confines of the computer facility.

3.2. Storage Protection

- Devise fire protection plans with data storage media in mind. Consider the risks which firefighting imposes on stored data. Tape and disk library vaults (safes) can be certified to have a particular protection rating and design which keeps contents safe from steam and water damage as well as from heat and flame. These ratings should be considered in evaluating and selecting storage facilities.
- Include protective measures in planning for disaster response. Disaster recovery procedures should be periodically tested and exercised. Arrangements should be made for the removal to a place of safekeeping of storage media, computer printouts, records of disclosure and source material. If potential threats of looting and pilfering exist, guards should be posted; if data is vulnerable to water damage, protective plastic covers should be available.
- To ensure that protection of data is adequately maintained, conduct frequent unscheduled security inspections. Check for unlocked doors, doors propped open, locks which do not latch, and fire and intrusion alarms which have been turned off because they are too easily activated.

Physical security measures are the first line of defense against the risks which stem from the uncertainties in the environment as well as from the unpredictability of human behavior. Frequently, they are the simplest safeguards to implement and can be put into practice with the least delay. Naturally, not all physical security measures are required at any one installation, but rather a judicious selection which provides a realistic overall coverage for the lowest expenditure.

4. Information Management Practices

Information management practices refer to those techniques and procedures used to control the many operations performed on information to accomplish the agency's objectives, but do not extend to the essential managerial determination of the need for and uses of information in relation to any agency's mission. In this context, information management includes: data collection, validation and transformation; information processing or handling; record keeping; information control, display, and presentation; and finally standardization of information management operations.

Effective application of these processes contributes importantly to the Privacy Act objectives of maintaining accurate, timely and complete data. An examination of current practices should, therefore, be a first order of business to determine whether modifications or enhancements are needed. Changes to current practices will be implemented with differing degrees of additional expense and operational overhead depending upon the extent to which good management practices already exist.

The information management guidelines presented below are grouped into major categories to facilitate the explanation of their role. *Every practice presented may not be required at every data processing installation.* Selection of practices for implementation from those identified below should reflect their relevance to the specific agency environment. For instance, an installation which processes only personal data could elect not to label volumes of storage media containing personal data.

4.1. Handling of Personal Data

- Prepare a procedures handbook which describes the precautions to be used and obligations of computer facility personnel during the physical handling of all personal data. Include a reference regarding the applicability of the procedures to those government contractors who are subject to the Privacy Act.
- Label all recording media which contain personal data. Labelling such media will reduce the probability of accidental abuse of such data, and also will aid in fixing the blame in the event of negligent or willfully malicious abuse.
- Store personal data in a manner that conditions users to respect its confidentiality; e.g., under lock and key when not being used.
- If a program generates reports containing personal data, have the program print clear warnings of the presence of such data on the reports.
- Color code all computer input/output card trays, tape reels, disk pack covers, etc., which contain personal data, so that they can be afforded the special protection required by law.
- Keep a record of all categories of personal data contained in computer-generated reports to facilitate compliance with the requirements that agencies identify all such data files and their routine use by the agency.
- Carefully control products of intermediate processing steps, e.g., scratch tapes and disk packs, to ensure that they do not contribute to unauthorized disclosure of personal data.
- Maintain an up-to-date hard copy authorization list of all individuals (computer personnel as well as system users) allowed to access personal data for use in access control and authorization validation. Operations and systems personnel should be considered privy to any data they handle since anomolous conditions may cause or require their knowledge of data contents.
- Maintain an up-to-date hard copy data dictionary listing the complete inventory of personal data files within the computer facility in order to account for all obligations and risks.

4.2. Maintenance of Records to Trace the Disposition of Personal Data

- Establish procedures for maintaining correct, current accounting of all new personal data brought into the computer facility.
- Log each transfer of storage media containing personal data to or from the computer facility.
- Maintain logbooks for terminals that are used to access personal data by system users.

4.3. Data Processing Practices

- Use control numbers to account for personal data upon receipt and during input, storage and processing.
- Verify the accuracy of personal data acquisition and entry methods employed.
- Take both regular and unscheduled inventories of all tape and disk storage media to ensure accurate accounting for all personal data.
- Use carefully-devised back-up procedures for personal data. A copy of the data should be kept at a second location if its maintenance is required by law.
- Create a records retention timetable covering all personal data and stating minimally, the data type, the retention period, and the authority responsible for making the retention decision.
- After a computer failure, check all personal data which was being processed at the time of failure for inaccuracies resulting from the failure.

- If the data volumes permit economic processing, some sensitive applications may use a dedicated processing period.
- Files created from files known to contain personal data should be examined to ensure that they cannot be used to regenerate any personal data. A formal process must be established for the determination and certification that such files are releasable in any given instance.
- In aggregating data, give consideration to whether the consequent file has been increased in value to a theft-attracting level.
- When manipulating aggregations and combinations of personal data, make impossible the tracing of any information concerning an individual. Steps should be taken such that no inference, deduction, or derivation processes can be used to recover personal data.

4.4. Programming Practices

- Subject all programming development and modification to independent checking by a second programmer, bound by procedural requirements developed by a responsible supervisor.
- Inventory current programs which process or access personal data; verify their authorized usage.
- Enforce programming practices which make the use of personal data in any computer program clearly and fully identified.*
- Strictly control and require written authorization for all operating system changes that involve software security.

4.5. Assignment of Responsibilities

- Make a designated individual responsible for examining installation practices in storage, use and processing of personal data, including the use of physical security measures, information management practices and computer system access controls. He should consider both internal uses and the authorized external transfer of data, reporting any risks to the relevant management authority.
- Make a designated individual responsible during each processing period (shift) for insuring that the facility is adequately manned with competent personnel and that the policies for the protection of personal data are enforced.

* See Section 6.5 of the "Guidelines for ADP Physical Security and Risk Management," referenced in the Appendix.

- Ensure that all employees engaged in the handling or processing of personal data adhere to established codes of conduct.

4.6. Procedural Auditing

Whenever appropriate, conduct an independent examination of established procedures. Audits of both specific information flow and general practices are possible. The following points should be considered when developing an audit:

- Auditing groups can be established within organizations to provide assurance of compliance independent of those directly responsible.
- Independent outside auditors can be contacted to provide similar assurance at irregular intervals.
- Audit reports should be maintained for routine inspection and to provide additional data for tracing compromises of confidentiality.

5. Systems Security

Once physical security measures and information management practices have been established, managers of some large information systems will want to consider system-based methods for protecting data. These include user identification procedures, access auditing to trace activity in the system, and system mechanisms to control data access, all of which can be incorporated into today's systems. Some details of these methods and the situations to which they are applicable are described here.

5.1. Identification

The identification of each individual who is allowed to use a system is a necessary step in safeguarding the data contained in that system. Identification of users is in many instances actually a two-step process consisting of identification and authentication, i.e. a would-be user of a system states who he is and the system verifies that he is who he claims to be. Determination of identity can range from the personal recognition by a system employee of a user submitting a batch job to a fully automated system log-on procedure from a remote terminal. The chance for misidentification is much greater when jobs are submitted directly into an ADP facility from a remote site and this chance is increased when access to the facility is achieved over common carrier lines.

There are three categories of methods by which a person's identity may be established for the purpose of allowing access to an information system. The methods, which can be applied singly or in combination, are based on:

- (1) Something the person *knows*;
- (2) Something the person *has*;
- (3) Something the person *is*.

The first category includes such things as passwords, the combinations to locks, or series of facts from an individual's personal background. The second category comprises such things as badges, cards with machine-readable information, and keys to locks. The third category consists of characteristics, such as a person's appearance, fingerprints, hand geometry, voice or signature. Identification based on "something a person is" includes recognition by guards, which is frequently the best defense against unauthorized access.

Badges, cards with machine readable information, or keys can be used for identification of users at terminals in remote locations, but some additional authentication procedure should also be considered. The physical security and procedural control of badges and keys, which frequently play a significant part in the identification process, are discussed in Section 3.1.

Passwords are perhaps today's most widely used identification technique for granting system access. They can be used to relate system users with specific system resources to which they are authorized access; they are also frequently associated with particular applications or information files. Because of their widespread use, considerable experience has been developed in the use of passwords. Considerations include:

- Passwords should be attributable to individuals in order to ascribe individual responsibility and reduce the likelihood of individuals giving out passwords to unauthorized coworkers. Passwords can be used not only to identify users, but also to control which data and other system resources they are authorized to use (see Section 5.2).
- Passwords should be easy to remember, but they should not be based on information such as a person's initials or birth date. It is best if the system administrators generate random passwords for users.
- Passwords should be changed at given intervals as well as whenever compromise is known or suspected.

5.2. System Access Controls

While identification can go a long way toward

preventing unauthorized use of a system, it is still necessary to have limitations on the use of data. Access controls can serve that purpose. They are the means of preventing a user, once having gained access to the system, from reading, altering or destroying any data he wishes. Lists (or even classes) of users authorized to perform certain activity or to access specified data or combinations of the two can be developed and stored in the computer to insure that only authorized data activity occurs.

Implementation considerations are:

- Some commercially available systems already have data access controls built in. In many cases these controls are not being used because some additional effort is sometimes required in reprogramming current applications. However, if needed, such access controls could provide a significant increase in data protection.
- Applications programs can have their own access control mechanisms built in if the operating system does not provide them.

5.3. Access Auditing

Closely allied to the access control mechanism is the ability to account for *who* had access to *which* data. The control mechanisms form the basis for reports on data usage. These reports, known as audit trails, can be designed to list all system activity, all data accesses, unusual activity, etc. Such a report can be examined for unauthorized disclosures of data.

The same auditing capability which produces the above reports can be used to enhance the automated log of system use presently utilized for charge accounting. Some benefits of such use may partially offset the costs of implementing the access control mechanism. A security log and audit will result in the recovery of some costs due to the more accurate charging for system use, better determination of causes of system failures, and, when properly exploited, greater facility for data base recovery in case of failure.

5.4. Network Systems

Risks to computer data become more significant during transmission among computer systems in a network or between a computer data bank and remote terminals. The potential of intentional compromise increases with the amount of data accessible in a network, the number of possible users of that data, and the geographic distribution of the network. In particular, there is the possibility that data may be intercepted while it is being transmitted. Also, messages may be modified or others substituted,

and false identities may be claimed by unauthorized network users or terminals. Finally, addresses may be accidentally or intentionally changed, sending traffic to the wrong destinations.

Although a proposed Federal standard for encryption is presently being prepared, it is neither presently available nor necessarily justified for protecting transfers of personal data. For the convenience of designers of future systems; encryption is discussed in Section 5.5.2. However, other steps for protection of data in networks are possible. Suggested considerations are:

- Establish requirements for identification, access control and access auditing methods in networks as in any other systems.
- Establish controls on network access. A useful procedure is to draw a diagram of the computer network architecture specifying the locations of all components (computers, terminals, communication paths). Each component should be labeled with a unique identifier, and a list of the people and terminals authorized to use the network should be prepared. For each, the list should include: identifier, terminals authorized for use, data access privileges and access restrictions. Rules for modifying this list, adding and deleting individuals or access privileges, should be developed.
- Log transfers of personal data in a security audit trail to account for disclosures of data.
- Verify special requests involving sensitive data to the computer operating system even though initial system access has been granted to the requestor.
- Assign a network security officer.

5.5. Planning for Future ADP Systems

It is important for those involved in planning future systems to be aware of forthcoming technological developments in computer security in order that the new technology can be incorporated into the design of the systems from their inception. The following discussions are offered for this reason.

5.5.1. Internal Controls

Current computer technology does not provide provable solutions to certain internal system security problems. These security problems arise from the fact that indirect and sophisticated penetration can bypass any ad hoc security controls. While this kind of security

problem exists, it is important not to overestimate its probability of occurrence. Such an attack will occur only when a skilled individual is motivated to dedicate an extensive effort to planning a deliberate penetration of an ADP system, and historically the motivation has been financial. The various system safeguards previously discussed will make it more difficult to plan and carry out an indirect attack. Security logs may be the most effective in deterring such attacks as they raise the probability of detecting the attack and of apprehending the attacker. It may not be cost-effective to provide additional safeguards specifically to counter sophisticated indirect attacks, such as penetration of an operating system.

Advancing technology may soon lead to very cost-effective protection against attempts to bypass internal system access controls. Those who will not be procuring computer systems until the late 70's or early 80's may be able to take advantage of such technology if the current research in this area is successful.

In the meantime, the following guidance is provided for current and future data processing installations which are dependent on current computer technology.

- Segment the data processing activity in such a way that the sensitive information is not totally available, nor vulnerable, at any one time or place.
- Personal data which may be subjected to intensive computer security threats should be processed with stringent physical and information management controls which provide the needed security; for example, the data could be processed in a dedicated mode or remote programming access to the system could be restricted during the processing of this information.

5.5.2. Data Encryption

The planning and design of a data processing network should provide safeguards so that no one can utilize the communication facilities to obtain sensitive information being transmitted through the network. Under certain circumstances of high risk, data encryption may be needed for the protection of personal data in computer networks. The following material is presented as background information for the planners of future networks.

Encryption is achieved either through a secret process or through a commonly known process which depends on a secret parameter. In order to allow compatibility of encryption processes within the typical variety of network compo-

nents, the latter method is preferred. The encryption process is generally specified in an algorithm (a set of rules or steps for performing a task) and the secret parameter supplied to the algorithm is called the key. Decryption is the inverse process.

The National Bureau of Standards published an encryption algorithm in the *Federal Register* of March 17, 1975, which satisfies the primary technical requirements of a data encryption standard. It is planned that this standard will be promulgated as a Federal Information Processing Standard (FIPS). The algorithm may be implemented in presently available electronic technology.

Control devices must be constructed to format the data for the encryption device and to transmit and receive the encrypted data. These will depend on the computer component and the communication network to which it is attached.

Identification, access control and access auditing should be implemented within a computer system before sophisticated encryption devices are procured for the protection of data in networks. However, assuming a defined need for encryption and the availability of encryption devices and any necessary network control devices, the following should be considered:

- Using the network diagram and the authorization list described in Section 5.4, the diagram should be augmented by locating encryption devices so as to protect personal data at places where data is vulnerable to network security threats.
- Data encryption keys must be created and distributed to authorized network personnel. They must be protected at all times and changed frequently. Periodic changes are suggested and immediate changes are necessary if a compromise has occurred or is thought to have occurred.

Appendix

Computer Security and Privacy Publications of the Institute for Computer Sciences and Technology

National Bureau of Standards

Title	Abstract	Source	Catalog No.	Cost
Controlled Accessibility Bibliography (NBS Technical Note 780; June, 1973)	A bibliography of works dealing with the hardware and software technological measures available in a computer system for the protection of data.	Superintendent of Documents U.S. Government Printing Office Washington, D.C. 20402	C13.46:780	\$.55
Controlled Accessibility Workshop Report (NBS Technical Note 827; May, 1974)	A report of the NBS/ACM Workshop on Controlled Accessibility, December 1972, Rancho Santa Fe, California. The workshop was divided into five separate working groups: access controls, audit, EDP management controls, identification, and measurements. The report contains the introductory remarks outlining the purpose and goals of the workshop, summaries of the discussions that took place in the working groups and the conclusions that were reached.	Superintendent of Documents U.S. Government Printing Office Washington, D.C. 20402	C13.46:827	\$1.25
Executive Guide to Computer Security (NBS Special Publication; May, 1974)	This booklet was prepared for non-ADP executives and managers. It is intended to introduce management to the necessity for computer security and the problems encountered in providing for it.	Systems and Software Division Room A247, Technology Building National Bureau of Standards Washington, D.C. 20234	None	No Charge
Guidelines for Physical Security and Risk Management (Federal Information Processing Standards Publication 31; June, 1974)	This publication provides guidelines to be used by Federal organizations in structuring physical security programs for their ADP facilities. It treats risk analysis, natural disasters, supporting utilities, system reliability, procedural measures and controls, off-site facilities, contingency plans, security awareness and security audit. Statistics and information relevant to physical security of computer data and facilities are presented. There are also many references to other, applicable publications containing more exhaustive treatments of specific subjects.	Superintendent of Documents U.S. Government Printing Office Washington, D.C. 20402	C13.52:31	\$1.35

APPENDIX H

APPLICABILITY CRITERIA FOR CERTIFICATION DETERMINATION

APPLICABILITY CRITERIA FOR CERTIFICATION DETERMINATION

Find the column that characterizes each agency in terms of the four applicability criteria, then read down the column to find the level of certification required.

APPLICABILITY CRITERIA:	Possible Combinations of Applicability Criteria												
	1	2	3	4	5	6	7	8	9	10	11	12	13
Agency received LEAA funds for CHRI	No	No	No	No	No	No	No	Yes	Yes	Yes	Yes	Yes	Yes
Agency collects/maintains CHRI	No	Yes	Yes	No	Yes	Yes	No	No	Yes	No	Yes	Yes	Yes
Agency disseminates CHRI	No	No	Yes	No	No	Yes	Yes	No	No	Yes	No	Yes	Yes
Agency receives CHRI	No	No	No	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	No	Yes
Totally unaffected by regulations				Required to comply only as specified in CHRI Use Agreement (existing or required to be developed)					1	2	3	4	5
									Required to complete certification process for appropriate situation				

APPENDIX I

CERTIFICATION APPLICABILITY CRITERIA

DETERMINATION SURVEY FORMS

- . Cover letter from Office of Court Administrator sent to all Courts
- . LEAA Regulations Applicability Determination Survey sent to all Courts
- . Cover letter from Chiefs of Police Association sent to all police departments
- . Cover letter from Sheriffs' Association sent to all sheriffs departments
- . Cover letter from Statewide Association of Prosecutors sent to all prosecutors
- . LEAA Regulations Applicability Determination Survey sent to all other agencies

OFFICE OF THE COURT ADMINISTRATOR
STATE OF UTAH

250 EAST BROADWAY, SUITE #240
SALT LAKE CITY, UTAH 84111
TELEPHONE: 328-6371

October 7, 1975

Mr. E. Royden Christian
Washington County Clerk
Box 579
St. George, Utah 84770

Dear Mr. Christian:

You may have heard that some activity was taking place regarding Security and Privacy and the handling of Criminal History Record information (CHRI). On May 20, 1975, the Law Enforcement Assistance Administration issued regulations requiring, among other things, that all states develop a Criminal History Record Information Privacy and Security Plan. This plan must set forth operational procedures to provide for the security and privacy of criminal history record information that will comply with the regulation. Those procedures must be operational in varying stages by December 16, 1977. The plan must be submitted to LEAA by December 16, 1975.

Govenor Rampton has indicated his support for the need for this plan, and has asked the Commissioner of the Department of Public Safety, Raymond A. Jackson, to proceed with its development. Commissioner Jackson has formed a Criminal History Privacy and Security Committee to oversee the plan's development and to advise the Law Enforcement Planning Agency which is directing the actual writing of the plan. The representative committee is presently composed of the following members:

Raymond A. Jackson: Commissioner, Department of Public Safety
Commissioner Harold Smith: Chairman, Govenors Council on Community Affairs
Vernon B. Romney: Attorney General
John McNamara: Administrator, Juvenile Court
Ernest D. Wright: Director, Department of Corrections
Arthur G. Christean: Court Administrator's Office
J. Leon Sorensen: Director, Legislative Research
Leo L. Memmott: Legislative Analyst
Robert B. Andersen: Director Law Enforcement Planning Agency

Page 2
October 7, 1975

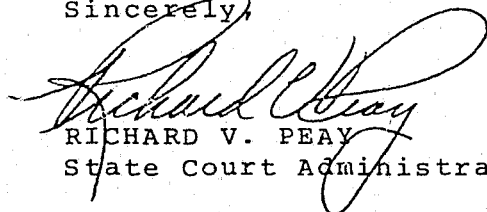
Ivard R. Rogers: Director, Bureau of Criminal
Identification
Wayne D. Shepherd: President, Chief's of Police
Association
Dr. H. Roy Curtin: Director, State Information
Center
David S. Young: Statewide Association of Prosecutors
Sheriff Floyd L. Witt: President, Sheriff's Association

The first step in the process of developing the plan will be to determine current practices in each criminal justice agency regarding CHRI and the applicability of these new federal regulations to such agencies. In the regulations and the supplementary instructions which interpret the regulations, "courts" are included in the definition of "criminal justice agency". However, the direct applicability of the regulations on the courts is governed by other criteria, including the receipt of federal funds for the development of systems that "collect, store, or disseminate criminal history record information".

To cooperate in the development of this plan and to determine the extent of the applicability of the federal regulations to the courts of this state, you are requested to complete the enclosed brief survey form which has been prepared by the Utah Law Enforcement Planning Agency. Mail the completed survey form by October 31, 1975.

If you have any questions call Mr. Arthur G. Christean, Deputy Court Administrator on my staff or Mr. Art Hudachko at the Utah Law Enforcement Planning Agency 533-5731.

Sincerely,


RICHARD V. PEAY
State Court Administrator

dj

Enclosure

cc Judge Joseph H. Burns

LEAA REGULATIONS APPLICABILITY DETERMINATION SURVEY

(YOUR AGENCY)

(YOUR NAME)

(DATE)

RETURN THIS FORM TO:

Mr. Art Hudachko
Law Enforcement Planning Agency
304 State Office Building
Salt Lake City, Utah 84114

Telephone: 533-5731

Mr. Hudachko may be contacted should you have any questions about how to complete the survey form.

Place an "X" in the YES or NO box opposite each question as it applies to your agency.

- | | <u>YES</u> | <u>NO</u> |
|---|--------------------------|--------------------------|
| 1. Has your agency received any LEAA funds for the development of manual or automated criminal history record information systems since July 1, 1973? | <input type="checkbox"/> | <input type="checkbox"/> |
| 2. Does your agency collect, store, and maintain criminal history and record information? | <input type="checkbox"/> | <input type="checkbox"/> |
| 3. Does your agency disseminate criminal history record information? | <input type="checkbox"/> | <input type="checkbox"/> |
| 4. Does your agency receive criminal history record information from other criminal justice or non-criminal justice agencies? | <input type="checkbox"/> | <input type="checkbox"/> |

The following definitions will be useful in interpreting the above questions as they apply to your agency:

1. 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 on such as fingerprint records to the extent that such information does not indicate involvement of the individual in the criminal justice system.

2. 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.
3. The regulations do 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 compiled chronologically; (4) published court opinions or public judicial 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 operator's licenses; (6) announcements of executive clemency.
4. Dissemination means release of criminal history record information by an agency (court) to another agency or individual. However, reporting of an arrest or other transaction (adjudication) to a state or local repository or another criminal justice agency so subsequent criminal justice proceedings can go forward is not considered dissemination. (Supplement No. 1 to Privacy and Security Instructions dated August 20, 1975).

COURT RECORDS

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

The purpose of this exception is to permit access to records which traditionally have been open to the public, defendants, or members of the bar. The basic model contemplated by the drafters is the register of cases maintained in most county clerk's offices. Entries are made in the registers as cases arise, and the outcomes of various motions, conferences, hearings and other stages of the adjudication are filed as they occur. Also included under this exception would be individual case files containing the trial transcript and other records accumulated in the course of the case. One important caveat, however, must be issued. "Rap sheets" or summary criminal histories are sometimes included in such files, as a matter of administrative practice in filing. These documents are not considered "court records" under this section and are not exempt from coverage under the regulations.

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

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

The regulations apply to combinations of any non-chronological index and file which might be used to assemble or permit retrieval of a summary criminal history on an individual. If as a result of automatic data processing, the equivalent to an alphabetical manual index exists, such automated files would likewise be subject to the regulations. (Supplement No. 2 to Privacy and Security Instructions dated September 30, 1975).



11



12





STATE OF UTAH CHIEFS OF POLICE ASSOCIATION

October 6, 1975

Dear Chief:

You have no doubt heard that there was some activity taking place in the state regarding Criminal History Record Information (CHRI) and Privacy and Security. On May 20, 1975, LEAA issued regulations requiring all states to develop a Criminal Record Information Privacy and Security Plan. This plan must set forth operational procedures to provide for the privacy and security of criminal history record information, and these procedures must be operational (in varying degrees) in all criminal justice agencies affected by the regulations by December 16, 1977.

Governor Rampton has indicated his support for the need for this plan, and has asked the Commissioner of the Department of Public Safety to proceed with the development and implementation of the plan. Commissioner Raymond A. Jackson has formed a Criminal History Privacy and Security Committee to oversee the plan's development and to advise the Law Enforcement Planning Agency who is directing the writing of the plan. This committee was formed to provide representation from all sectors of the criminal justice community and is composed of the following members:

Raymond A. Jackson: Commissioner, Department of Public Safety
Commissioner Harold Smith: Chairman, Governors Council on
Community Affairs
Vernon B. Romney: Attorney General
John McNamara: Administrator, Juvenile Court

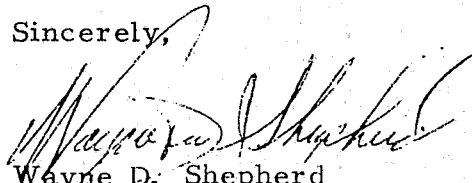
Chief of Police
October 6, 1975
Page 2

Ernest D. Wright: Director, Department of Corrections
Arthur G. Christean: Court Administrator's Office
Leon Sorensen: Director, Legislative Research
Leo L. Memmott: Legislative Analyst
Robert B. Andersen: Director, Law Enforcement Planning Agency
Ivard R. Rogers: Director, Bureau of Criminal Identification
Wayne D. Shepherd: President, Chiefs of Police Association
Dr. H. Roy Curtin: Director, State Information Center
David S. Young: Statewide Association of Prosecutors
Sheriff Floyd L. Witt: President, Sheriffs Association

The first step in the process of developing the plan is to determine current practices in each criminal justice agency as it relates to criminal history record information. Enclosed is a survey form which we encourage you to complete. It will only take a minute, and it will save time later on in the planning effort by eliminating the need to call your agency for the information. A stamped envelope is enclosed for your convenience.

If you have any questions, please give me a call; or call Mr. Art Hudachko at the Utah State Law Enforcement Planning Agency, 533-5731.

Sincerely,



Wayne D. Shepherd
President

Enclosures:
Survey
Envelope

UTAH SHERIFFS' ASSOCIATION

FLOYD L. WITT
PRESIDENT



Dear Sheriff:

You have no doubt heard that there was some activity taking place in the state regarding Criminal History Record Information (CHRI) and Privacy and Security. On May 20, 1975, LEAA issued regulations requiring all states to develop a Criminal History Record Information Privacy and Security Plan. This plan must set forth operational procedures to provide for the privacy and security of criminal history record information, and these procedures must be operational (in varying degrees) in all criminal justice agencies affected by the regulations by December 16, 1977.

Governor Rampton has indicated his support for the need for this plan, and has asked the Commissioner of the Department of Public Safety to proceed with the development and implementation of the plan. Commissioner Raymond A. Jackson has formed a Criminal History Privacy and Security Committee to oversee the plan's development and to advise the Law Enforcement Planning Agency who is directing the writing of the plan. This committee was formed to provide representation from all sectors of the criminal justice community and is composed of the following members:

Raymond A. Jackson: Commissioner, Department of Public Safety

Commissioner Harold Smith: Chairman, Governors Council on Community Affairs

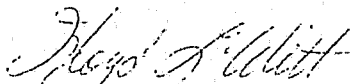
David S. Young: Statewide Association of Prosecutors

Wayne D. Shepherd: President, Chief's of Police Association
Sheriff Floyd L. Witt: President, Sheriffs' Association
Dr. H. Roy Curtin: Director, State Information Center
Leo L. Memmott: Legislative Analyst
Ernest D. Wright: Director, Department of Corrections
John McNamara: Administrator, Juvenile Court
Arthur G. Christean: Court Administrator's Office
Ivard R. Rogers: Director, Bureau of Criminal Identification
Vernon B. Romney: Attorney General
Robert B. Anderson: Director, Law Enforcement Planning Agency
Leon Sorensen: Director, Legislative Research

The first step in the process of developing the plan is to determine current practices in each criminal justice agency as it relates to criminal history record information. Enclosed is a survey form which we encourage you to complete. It will only take a minute, and it will save time later on in the planning effort by eliminating the need to call your agency for the information. A stamped envelope is enclosed for your convenience.

If you have any questions, please give me a call; or call Mr. Art Hudachko at the Utah State Law Enforcement Planning Agency, 533-5731.

Sincerely,



Floyd L. Witt, President
Utah Sheriffs' Association

FLW:vp

Enclosures:
Survey
Envelope



STATEWIDE
ASSOCIATION OF PROSECUTORS
OF UTAH

ADVISORY BOARD
R. PAUL VAN DAM, CHAIRMAN
K. L. McIFF
HANS Q. CHAMBERLAIN
J. DUFFY PALMER
BURTON H. HARRIS
MERRILL HANSEN
VERNON B. ROMNEY

220 SOUTH SECOND EAST, SUITE 440
SALT LAKE CITY, UTAH 84111
TELEPHONE (801) 532-8503

DAVID S. YOUNG
DIRECTOR

LARRY V. SPENDLOVE
ASSISTANT DIRECTOR

M. REID RUSSELL
DIRECTOR, TECHNICAL
ASSISTANCE BUREAU

October 7, 1975

Dear Prosecutor:

You have no doubt heard that there was some activity taking place in the state regarding Criminal History Record Information (CHRI) and Privacy and Security. On May 20, 1975, LEAA issued regulations requiring all states to develop a Criminal History Record Information Privacy and Security Plan. This plan must set forth operational procedures to provide for the privacy and security of criminal history record information, and these procedures must be operational (in varying degrees) in all criminal justice agencies affected by the regulations by December 16, 1977.

Governor Rampton has indicated his support for the need for this plan, and has asked the Commissioner of the Department of Public Safety to proceed with the development and implementation of the plan. Commissioner Raymond A. Jackson has formed a Criminal History Privacy and Security Committee to oversee the plan's development and to advise the Law Enforcement Planning Agency who is directing the writing of the plan. This committee was formed to provide representation from all sectors of the criminal justice community and is composed of the following members:

Raymond A. Jackson: Commissioner, Department of Public Safety
Commissioner Harold Smith: Chairman, Governors Council on
Community Affairs
Vernon B. Romney: Attorney General
John McNamara: Administrator, Juvenile Court
Ernest D. Wright: Director, Department of Corrections
Arthur G. Christean: Court Administrator's Office
Leon Sorensen: Director, Legislative Research
Leo L. Memmott: Legislative Analyst
Robert B. Andersen: Director, Law Enforcement Planning Agency
Ivard R. Rogers: Director, Bureau of Criminal Identification

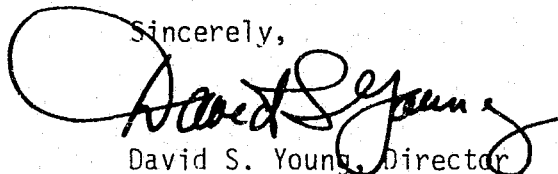
Prosecutor
October 7, 1975
Page 2

Wayne D. Shepherd: President, Chiefs of Police Association
Dr. H. Roy Curtin: Director, State Information Center
David S. Young: Director, Statewide Association of Prosecutors
Sheriff Floyd L. Witt: President, Sheriffs Association

The first step in the process of developing the plan is to determine current practices in each criminal justice agency as it relates to criminal history record information. Enclosed is a survey form which we encourage you to complete. It will only take a minute, and it will save time later on in the planning effort by eliminating the need to call your agency for the information.

If you have any questions, please give me a call; or call Mr. Art Hudachko at the Utah State Law Enforcement Planning Agency, 533-5731.

Sincerely,

A handwritten signature in black ink, appearing to read "David S. Young", written over a large, loopy circular flourish.

David S. Young, Director
Statewide Association of Prosecutors

Enclosure

LEAA REGULATIONS APPLICABILITY DETERMINATION SURVEY

(YOUR AGENCY)

(YOUR NAME)

(DATE)

RETURN THIS FORM TO:

Return by October 31, 1975

Mr. Art Hudachko
Law Enforcement Planning Agency
304 State Office Building
Salt Lake City, Utah 84114

Telephone: 533-5731

Mr. Hudachko may be contacted should you have any questions about how to complete the survey form.

Place an "X" in the YES or NO box opposite each question as it applies to your agency.

- | | <u>YES</u> | <u>NO</u> |
|---|--------------------------|--------------------------|
| 1. Has your agency received any LEAA funds for the development of manual or automated criminal history record information systems since July 1, 1973? | <input type="checkbox"/> | <input type="checkbox"/> |
| 2. Does your agency collect, store, and maintain criminal history and record information? | <input type="checkbox"/> | <input type="checkbox"/> |
| 3. Does your agency disseminate criminal history record information? | <input type="checkbox"/> | <input type="checkbox"/> |
| 4. Does your agency receive criminal history record information from other criminal justice or non-criminal justice agencies? | <input type="checkbox"/> | <input type="checkbox"/> |

The following definitions will be useful in interpreting the above questions as they apply to your agency:

1. 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 on such as fingerprint records to the extent that such information does not indicate involvement of the individual in the criminal justice system.

CONTINUED

2 OF 4

2. 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.
3. The regulations do 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 compiled chronologically; (4) published court opinions or public judicial 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 operator's licenses; (6) announcements of executive clemency.

APPENDIX J

AGENCY LIST/CERTIFICATION PROCESS

REQUIREMENT CHECKLISTS



STATE AGENCIES
AGENCY LIST/CERTIFICATION PROCESS REQUIREMENT

AGENCY IDENTIFICATION	Applicability Criteria No.	CERTIFICATION PROCESS REQUIRED						
		Unaffected by Regulations	Use Agreement Required	Must complete certifica- tion process:				
				1	2	3	4	5
STATE AGENCIES								
Attorney General	5		x					
Division of Corrections	13							x
Juvenile Court	13							x
Liquor Law Enforcement	6		x					
Office of Court Administrator	1	x						
Peace Officer Standards and Training	4		x					
Utah Bureau of Criminal Identification	13							x
Utah Highway Patrol	7		x					

SHERIFF'S OFFICES
AGENCY LIST/CERTIFICATION PROCESS REQUIREMENT

AGENCY IDENTIFICATION	Applicability Criteria No.	CERTIFICATION PROCESS REQUIRED							
		Unaffected by Regulations	Use Agreement Required	Must complete certifica- tion process:					
				1	2	3	4	5	
SHERIFF'S OFFICES									
Beaver County	6		x						
Box Elder County	6		x						
Cache County	3	x							
Carbon County	3	x							
Daggett County	6		x						
Davis County	13								x
Duchesne County	6		x						
Emery County	2	x							
Garfield County	6		x						
Grand County	5		x						
Iron County	6		x						
Juab County	2	x							
Kane County	5		x						
Millard County	6		x						
Morgan County	6		x						
Piute County	6		x						
Rich County	6		x						
Salt Lake County	13								x
San Juan County	6		x						
Sanpete County	2	x							
Sevier County	6		x						
Summit County	6		x						
Tooele County	6		x						
Uintah County	6		x						
Utah County	13								x
Wasatch County	6		x						
Washington County	4		x						
Wayne County	2	x							
Weber County	6		x						

POLICE DEPARTMENTS
AGENCY LIST/CERTIFICATION PROCESS REQUIREMENT

AGENCY IDENTIFICATION	Applicability Criteria No.	CERTIFICATION PROCESS REQUIRED						
		Unaffected by Regulations	Use Agreement Required	Must complete certifica- tion process:				
				1	2	3	4	5
POLICE DEPARTMENTS								
American Fork	6		x					
Aurora	1	x						
Beaver	1	x						
Blanding	2	x						
Bloomington	1	x						
Bountiful	13							x
Brigham City	13							x
Brigham Young University	6		x					
Cedar City	6		x					
Centerville	6		x					
Clearfield	5		x					
Clinton	4		x					
Delta	6		x					
Dixie College	6		x					
Duchesne	6		x					
Ephraim	1	x						
Eureka	1	x						
Farmington	2	x						
Fillmore	6		x					
Fort Duchesne	1	x						
Green River	1	x						
Gunnison	1	x						
Helper	6		x					
Henefer	1	x						
Hurricane	6		x					
Hyde Park	6		x					
Hyrum	5		x					
Kanab	6		x					
Kanarraville	1	x						
Kaysville	6		x					
Layton	6		x					
Lehi	6		x					
Lewiston	1	x						
Lindon	1	x						
Logan	6		x					
Manti	4		x					
Mantua	1	x						
Mapleton	1	x						
Midvale	5		x					
Milford	1	x						

POLICE DEPARTMENTS
AGENCY LIST/CERTIFICATION PROCESS REQUIREMENT

AGENCY IDENTIFICATION	Applicability Criteria No.	CERTIFICATION PROCESS REQUIRED						
		Unaffected by Regulations	Use Agreement Required	Must complete certifica- tion process:				
				1	2	3	4	5
POLICE DEPARTMENTS - Continued								
Moab	2	x						
Monroe	2	x						
Monticello	6		x					
Morgan	3	x						
Mt. Pleasant	3	x						
Murray	13							x
Nephi	1	x						
North Logan	6		x					
North Ogden	5		x					
North Salt Lake	1	x						
Ogden	13							x
Orem	6		x					
Panguitch	6		x					
Paragonah	1	x						
Park City	6		x					
Parowan	6		x					
Payson	6		x					
Pleasant Grove	7		x					
Price	6		x					
Provo	13							x
Richfield	1	x						
Riverdale	5		x					
Roosevelt	6		x					
Roy	6		x					
St. George	6		x					
Salina	3	x						
Salt Lake	13							x
Sandy	6		x					
Santaquin	1	x						
South Ogden	6		x					
South Salt Lake	6		x					
Spring City	1	x						
Springville	6		x					
Sunset	6		x					
Syracuse	6		x					
Tooele	6		x					
Tremonton	6		x					
University of Utah	6		x					
Vernal	6		x					

POLICE DEPARTMENTS

AGENCY LIST/CERTIFICATION PROCESS REQUIREMENT

AGENCY IDENTIFICATION	Applicability Criteria No.	CERTIFICATION PROCESS REQUIRED							
		Unaffected by Regulations	Use Agreement Required	Must complete certifica- tion process:					
				1	2	3	4	5	
POLICE DEPARTMENTS - Continued									
Washington	6		x						
Washington Terrace	4		x						
Weber State College	6		x						
Wellington	5		x						
West Bountiful	5		x						
Woods Cross	6		x						

POLICE DEPARTMENTS
AGENCY LIST/CERTIFICATION PROCESS REQUIREMENT

CERTIFICATION PROCESS REQUIRED

AGENCY IDENTIFICATION

The following police departments
 did not return the certification
 form - continued

Applicability
Criteria No.

Unaffected by
Regulations

Use Agreement
Required

Must complete certifica-
tion process:

1 2 3 4 5

Oak City
 Oakley
 Orangeville
 Perry
 Plain City
 Plymouth
 Pleasant View
 Providence
 Randolph
 Redmond
 Riverton
 Salem
 Santa Clara
 Sigurd
 Snowville
 Southern Utah State College
 Spansih Fork
 Springdale
 Stockton
 Sunnyside
 Toquerville
 Tropic
 Uintah
 Virgin
 Wales
 Wellsville
 Wendover
 West Jordan
 Willard

JUSTICES OF THE PEACE
AGENCY LIST/CERTIFICATION PROCESS REQUIREMENT

AGENCY IDENTIFICATION	Applicability Criteria No.	CERTIFICATION PROCESS REQUIRED						
		Unaffected by Regulations	Use Agreement Required	Must complete certifica- tion process:				
				1	2	3	4	5
JUSTICES OF THE PEACE								
American Fork (2)	1	x						
Beaver City	6		x					
Beaver County	1	x						
Box Elder County	1	x						
Castle Dale	1	x						
Cedar City (2)	1	x						
	4		x					
Circleville	1	x						
Clinton	1	x						
Coalville	1	x						
Davis County	3	x						
Delta (2)	1	x						
Duchesne	1	x						
Dutch John	1	x						
East Layton	1	x						
Fillmore	2	x						
Garden City	2	x						
Glenwood	1	x						
Grantsville	4		x					
Harrisville	1	x						
Heber	2	x						
Kane County	4		x					
Kaysville	6		x					
Leeds	1	x						
Lehi (2)	4		x					
	2	x						
Meadow	1	x						
Midvale	6		x					
Midway	1	x						
Minersville	1	x						
Monroe	1	x						
Monticello	1	x						
Morgan (2)	1	x						
North Logan	1	x						
Park City	2	x						
Payson	2	x						
Pleasant Grove	1	x						
Pleasant View	1	x						
Providence	2	x						
Richfield	4		x					

JUSTICES OF THE PEACE
AGENCY LIST/CERTIFICATION PROCESS REQUIREMENT

AGENCY IDENTIFICATION	Applicability Criteria No.	CERTIFICATION PROCESS REQUIRED							
		Unaffected by Regulations	Use Agreement Required	Must complete certifica- tion process:					
				1	2	3	4	5	
JUSTICES OF THE PEACE - Continued									
Richmond	1	x							
River Heights	1	x							
Roosevelt (2)	1	x							
Salt Lake City	7		x						
San Juan County	1	x							
Sandy (2)	1	x							
	6		x						
North Sevier	1	x							
South Ogden	5		x						
Springdale	1	x							
Springville	1	x							
Stockton	4		x						
Sunset	4		x						
Tremonton	6		x						
Vernal (2)	1	x							
Washington	1	x							
Wellington	6		x						
Wellsville	1	x							
Woods Cross	4		x						
The following agencies did not return the certification forms									
Alpine									
Bicknell									
Blanding (2)									
Bluff									
Brigham City (2)									
Bullfrog Basin									
Centerville									
Clarkston									
Cleveland									
Corinne									
East Carbon City.									
Elsinor									
Emery									
Enterprise (2)									
Ephraim (2)									

JUSTICES OF THE PEACE
AGENCY LIST/CERTIFICATION PROCESS REQUIREMENT

AGENCY IDENTIFICATION	Applicability Criteria No.	CERTIFICATION PROCESS REQUIRED							
		Unaffected by Regulations	Use Agreement Required	Must complete certifica- tion process:					
				1	2	3	4	5	
The following justices of the peace agencies did not return the certification form - continued									
Moroni Mt. Carmel Mt. Pleasant Myton Nephi (3) Newton Nibley North Ogden North Salt Lake Ogden (2) Panguitch Paradise Paragonah Park City Parowan Payson Plain City Redmond Richfield Riverdale Riverton St. George (2) Salem Salina Salt Lake (3) Santa Clara Santaquin Smithfield Snowville Spanish Fork (2) Springville Sunnyside Syracuse Thompson Tooele Toquerville									

JUSTICES OF THE PEACE

AGENCY LIST/CERTIFICATION PROCESS REQUIREMENT

CERTIFICATION PROCESS REQUIRED

AGENCY IDENTIFICATION

The following justices of the peace agencies did not return the certification forms - continued

**Applicability
Criteria No.**

Unaffected by Regulations

**Use Agreement
Required**

Must complete certification process:

1

2

3

4

5

Torrey
Trenton
Tridell
Washington Terrace
Wendover
West Bountiful
West Jordan
Willard (2)
Woodruff

COURTS
AGENCY LIST/CERTIFICATION PROCESS REQUIREMENT

AGENCY IDENTIFICATION	Applicability Criteria No.	CERTIFICATION PROCESS REQUIRED							
		Unaffected by Regulations	Use Agreement Required	Must complete certifica- tion process:					
				1	2	3	4	5	
DISTRICT COURTS									
<u>District I (1 Court)</u>									
Box Elder County Clerk	1	x							
Cache County Clerk	5		x						
Rich County Clerk	5		x						
<u>District II (4 Courts)</u>									
Davis County Clerk	1	x							
Morgan County Clerk	2	x							
Weber County Clerk	3	x							
<u>District III (10 Courts)</u>									
Salt Lake County Clerk	6		x						
Tooele County Clerk	6		x						
<u>District IV (3 Courts)</u>									
Daggett County Clerk (No Response)									
Duchesne County Clerk	1	x							
Summit County Clerk	3	x							
Uintah County Clerk (No Response)									
Utah County Clerk	6		x						
Wasatch County Clerk	6		x						
<u>District V (1 Court)</u>									
Beaver County Clerk (No Response)									
Iron County Clerk	1	x							
Juab County Clerk	1	x							
Millard County Clerk (No Response)									
Washington County Clerk	1	x							

COURTS
AGENCY LIST/CERTIFICATION PROCESS REQUIREMENT

AGENCY IDENTIFICATION	Applicability Criteria No.	CERTIFICATION PROCESS REQUIRED							
		Unaffected by Regulations	Use Agreement Required	Must complete certifica- tion process:					
				1	2	3	4	5	
DISTRICT COURTS -continued									
<u>District VI (1 Court)</u>									
Garfield County Clerk (No Response)	1								
Kane County Clerk	1								
Piute County Clerk	1								
Sanpete County Clerk (No Response)									
Sevier County Clerk (No Response)									
Wayne County Clerk	1								
<u>District VII (1 Court)</u>									
Carbon County Clerk	5								
Emery County Clerk	2								
Grand County Clerk	5								
San Juan County Clerk	6								
NOTE: The county clerk acts as the ex-officio clerk of the district court									

COURTS

AGENCY IDENTIFICATION

CERTIFICATION PROCESS REQUIRED

**Applicability
Criteria No.**

Unaffected by Regulations

**Use Agreement
Required**

Must complete certification process:

1

2

3

4

5

CITY COURTS

CITY COURTS

Bountiful City Clerk (No Response)

Brigham City Clerk (No Response)

Clearfield City Clerk

Layton City Clerk (No Response)

Logan City Clerk (No Response)

Moab City Clerk

Murray City Clerk

ogden City Clerk

Orem City Clerk

Price City Clerk

Provo City Clerk

Roy City Clerk

Salt Lake City Clerk (No Response)

St. George City Clerk

Tooele City Clerk

NOTE: The city clerk acts as the
ex officio clerk of the
city court

ATTORNEYS

AGENCY LIST/CERTIFICATION PROCESS REQUIREMENT

AGENCY IDENTIFICATION	Applicability Criteria No.	CERTIFICATION PROCESS REQUIRED							
		Unaffected by Regulations	Use Agreement Required	Must complete certifica- tion process:					
				1	2	3	4	5	
ATTORNEYS									
COUNTY									
Beaver	1	x							
Box Elder	1	x							
Cache	4		x						
Carbon	5		x						
Daggett	1	x							
Davis	2	x							
Emery	1	x							
Garfield	5		x						
Grand	1	x							
Iron	1	x							
Juab	6		x						
Kane	5		x						
Millard	1	x							
Piute	2	x							
Rich	1	x							
Salt Lake	13								x
San Juan	4		x						
Sanpete	1	x							
Sevier	2	x							
Summit	4		x						
Uintah	1	x							
Utah	4		x						
Wasatch	1	x							
Washington	5		x						
Weber	4		x						
CITY									
Brigham	1	x							
Cedar City	6		x						
Fillmore	1	x							
Logan	4		x						
Midvale	6		x						
Ogden	1	x							
Provo	6		x						
Richfield	1	x							
Tooele	4		x						

ATTORNEYS

CERTIFICATION PROCESS REQUIRED

APPENDIX K
MASTER CERTIFICATION ELEMENTS

MASTER CERTIFICATION ELEMENTS

Page 1

OPERATIONAL PROCEDURE REQUIRED BY PRIVACY AND SECURITY PLAN	APPLICABILITY CRITERIA					
	9	10	11	12	13	13
	CERTIFICATION PROCESS					
	1	2	3	4	5	Central Repository (UBI)
A. <u>Completeness and Accuracy Procedures</u>						
1. Is there a State or local agency Central Repository?	X		X	X	X	X
a. Is there Statutory/Executive authority for the Central Repository?	X		X	X	X	X
b. Are facilities and staff adequate to provide CHRI services Statewide or locally?	X		X	X	X	X
2. Is there a disposition reporting system?				X	X	X
a. Is disposition reporting provided within 90 days from:						
1. Police				X	X	X
2. Prosecutors				X	X	X
3. Trial Courts				X	X	X
4. Appellate Courts				X	X	X
5. Correctional Institutions				X	X	X
6. Probation and Parole Agencies				X	X	X

Legend: x = applies to all agencies in every case
c = applies only to agencies who have their own computer systems

MASTER CERTIFICATION ELEMENTS

Page 2

OPERATIONAL PROCEDURE REQUIRED BY PRIVACY AND SECURITY PLAN	APPLICABILITY CRITERIA					
	9	10	11	12	13	13
	CERTIFICATION PROCESS					
	1	2	3	4	5	Central Repository (UBI)
b. Is there a Delinquent Disposition Monitoring System to provide for: <ol style="list-style-type: none"> Delinquent disposition monitoring One-year rule/dissemination without disposition Terminal output flags 	<div></div> <div></div> <div></div>	<div></div> <div></div> <div></div>	<div></div> <div></div> <div></div>	<div>X</div> <div>X</div> <div>X</div>	<div>X</div> <div>X</div> <div>X</div>	<div>X</div> <div>X</div> <div>X</div>
c. Is there a procedure to report disposition of arrests occurring after June 19, 1975 within the 90-day rule?	<div></div>	<div></div>	<div></div>	<div>X</div>	<div>X</div>	<div>X</div>
3. Are there procedures for repository query by criminal justice agencies before CHRI dissemination?	<div></div>	<div>X</div>	<div></div>	<div>X</div>	<div>X</div>	<div>X</div>
a. Are query requirements documented?	<div></div>	<div>X</div>	<div></div>	<div>X</div>	<div>X</div>	<div>X</div>
b. Are written agreements with user agencies in existence?	<div></div>	<div>X</div>	<div></div>	<div>X</div>	<div>X</div>	<div>X</div>
4. Are there procedures to maintain accuracy of records?	<div>X</div>	<div>X</div>	<div>X</div>	<div>X</div>	<div>X</div>	<div>X</div>
a. Is notification on inaccurate information provided?	<div></div>	<div>X</div>	<div></div>	<div>X</div>	<div>X</div>	<div>X</div>

Legend: x = applies to all agencies in every case
c = applies only to agencies who have their own computer systems

MASTER CERTIFICATION ELEMENTS

OPERATIONAL PROCEDURE REQUIRED BY PRIVACY AND SECURITY PLAN	APPLICABILITY CRITERIA					
	9	10	11	12	13	13
	CERTIFICATION PROCESS					
	1	2	3	4	5	Central Repository (UBI)
5. Are CHRI dissemination and manual file screening procedures in use with criminal history record systems other than the Central Repository (UBI)?	_____	X	_____	X	X	_____
B. <u>Limits on Dissemination Procedures</u>						
1. Are general policies on use and dissemination documented?	_____	X	_____	X	X	X
and						
Are there procedures restricting and limiting dissemination in the following situations:	_____	X	_____	X	X	X
a. Juvenile record dissemination	_____	X	_____	X	X	X
b. Confirmation of record existence	_____	X	_____	X	X	X
c. Secondary dissemination by non-criminal justice agencies	_____	X	_____	X	X	X
2. Are there sanctions for individuals and agencies authorized who violate CHRI dissemination policies?	_____	X	_____	X	X	X

Legend: x = applies to all agencies in every case
c = applies only to agencies who have their own computer systems

MASTER CERTIFICATION ELEMENTS

OPERATIONAL PROCEDURE REQUIRED BY PRIVACY AND SECURITY PLAN	APPLICABILITY CRITERIA					
	9	10	11	12	13	13
	CERTIFICATION PROCESS					
	1	2	3	4	5	Central Reposi- tory (UBI)
3. Are there procedures for validating agency right of access for:						
a. Criminal justice agencies	___	X	___	X	X	X
b. Non-criminal justice agencies	___	X	___	X	X	X
c. Service agencies under contract	___	X	___	X	X	X
d. Research organizations	___	X	___	X	X	X
e. Right of access validation	___	X	___	X	X	X
4. Are notices presented to agencies not directly subject to the regulations?	___	___	___	___	___	X
C. <u>Audits and Quality Control Procedures</u>						
1. Is there a systematic audit (quality controls) process providing:						
a. Audit trails	X	___	X	X	X	X
b. Accuracy checks	X	___	X	X	X	X
c. Random document and record inspection	X	___	X	X	X	X
d. Dissemination logs	___	X	___	X	X	X
2. Are annual audits/compliance reviews performed on:						
a. Central Repository (UBI)	___	___	___	___	___	X

Legend: x = applies to all agencies in every case
c = applies only to agencies who have their own computer systems

MASTER CERTIFICATION ELEMENTS

Page 5

OPERATIONAL PROCEDURE REQUIRED BY PRIVACY AND SECURITY PLAN	APPLICABILITY CRITERIA					
	9	10	11	12	13	13
	CERTIFICATION PROCESS					
	1	2	3	4	5	Central Reposi- tory (UBI)
b. Other state and local systems	—	—	—	—	—	X
c. Documents and data to be maintained	—	—	—	—	—	X
D. <u>Security and Confidentiality Procedures</u>						
1. Does the hardware and software provide for:						
a. General security provisions	C	C	C	C	C	X
b. Procedures for access	C	C	C	C	C	X
c. Dedication of:						
1. Terminals	C	C	C	C	C	X
2. Communications control	C	C	C	C	C	X
3. Processor	C	C	C	C	C	X
4. Storage devices	C	C	C	C	C	X
and does the software provide maximum security of CHRI?	C	C	C	C	C	X
2. Is there adequate management control and is a responsible agency designated to provide for:						
a. Management control and accountability	C	C	C	C	C	X

Legend: x = applies to all agencies in every case
c = applies only to agencies who have their own computer systems

MASTER CERTIFICATION ELEMENTS

Page 6

OPERATIONAL PROCEDURE REQUIRED BY PRIVACY AND SECURITY PLAN	APPLICABILITY CRITERIA					
	9	10	11	12	13	13
	CERTIFICATION PROCESS					
	1	2	3	4	5	Central Reposi- tory (UBI)
b. Computer operations policy	<u>C</u>	<u>C</u>	<u>C</u>	<u>C</u>	<u>C</u>	<u>X</u>
c. Access to criminal history records	<u>C</u>	<u>C</u>	<u>C</u>	<u>C</u>	<u>C</u>	<u>X</u>
d. Sanctions for misuse	<u>C</u>	<u>C</u>	<u>C</u>	<u>C</u>	<u>C</u>	<u>X</u>
3. Does the personnel process provide:						
a. Selection and security screening	<u>C</u>	<u>C</u>	<u>C</u>	<u>C</u>	<u>C</u>	<u>X</u>
b. Supervision	<u>C</u>	<u>C</u>	<u>C</u>	<u>C</u>	<u>C</u>	<u>X</u>
c. Training	<u>C</u>	<u>C</u>	<u>C</u>	<u>C</u>	<u>C</u>	<u>X</u>
4. Is there physical security to:						
a. Protect against environmental hazards	<u>C</u>	<u>C</u>	<u>C</u>	<u>C</u>	<u>C</u>	<u>X</u>
b. Prevent physical access by unauthorized personnel	<u>C</u>	<u>C</u>	<u>C</u>	<u>C</u>	<u>C</u>	<u>X</u>
c. Secure facilities construction	<u>C</u>	<u>C</u>	<u>C</u>	<u>C</u>	<u>C</u>	<u>X</u>

Legend: x = applies to all agencies in every case
c = applies only to agencies who have their
own computer systems

MASTER CERTIFICATION ELEMENTS

OPERATIONAL PROCEDURE REQUIRED BY PRIVACY AND SECURITY PLAN	APPLICABILITY CRITERIA					
	9	10	11	12	13	13
	CERTIFICATION PROCESS					
	1	2	3	4	5	Central Repository (UBI)
E. <u>Individual Right of Access Procedures</u>						
1. Are there adequate procedures to verify identity before releasing information?	<u>X</u>		<u>X</u>	<u>X</u>	<u>X</u>	<u>X</u>
2. Are the rules for access written and disseminated to the public?	<u>X</u>		<u>X</u>	<u>X</u>	<u>X</u>	<u>X</u>
3. Is there a specified and convenient point of review and mechanism for review of CHRI?	<u>X</u>		<u>X</u>	<u>X</u>	<u>X</u>	<u>X</u>

Legend: x = applies to all agencies in every case
c = applies only to agencies who have their own computer system

MASTER CERTIFICATION ELEMENTS

Page 8

OPERATIONAL PROCEDURE REQUIRED BY PRIVACY AND SECURITY PLAN	APPLICABILITY CRITERIA					
	9	10	11	12	13	13
	CERTIFICATION PROCESS					
	1	2	3	4	5	Central Reposi- tory (UBI)
4. Is there a procedure for an individual to challenge the accuracy of his or her CHRI?	X		X	X	X	X
5. Is there a process for administrative review and record correction?	X		X	X	X	X
6. Are appeal procedures clearly identified?	X		X	X	X	X
7. Are correction procedures clearly identified?	X		X	X	X	X
8. Is the information subject to review clearly identified?	X		X	X	X	X
9. Will procedures be operational by March 16, 1976 which allow an individual to access and review his or her CHRI?						X

Legend: x = applies to all agencies in every case
c = applies only to agencies who have their own computer systems

APPENDIX L
CERTIFICATION PROCEDURE

Date of Certification:

OPERATIONAL PROCEDURE REQUIRED
BY PRIVACY AND SECURITY PLAN

A procedure is operational and:

No procedure is operational

Reason that procedure
is not fully operational:

Procedure meets Plan requirements

Procedure does not meet Plan requirements

Cost constraints

Time constraints

Technological

Lack of Authority

Estimated date
for procedure to be
fully operational

A. Completeness and Accuracy Procedures

1. Is there a State or local agency Central Repository?
 - a. Is there Statutory/Executive authority for the Central Repository?
 - b. Are facilities and staff adequate to provide CHRI services Statewide or locally?
2. Is there a disposition reporting system?
 - a. Is disposition reporting provided within 90 days from:
 1. Police
 2. Prosecutors
 3. Trial Courts
 4. Appellate Courts
 5. Correctional Institutions
 6. Probation and Parole Agencies

AGENCY: _____

Date of Certification: _____

Person Conducting Certification

[illegible]

Date of Certification: _____

Person Conducting Certification

[illegible]

Date of Certification:

Person Conducting Certification

[illegible]

PROCESS NO. (1, 2, 3, 4, 5, CENTRAL REPOSITORY)

AGENCY: _____

Date of Certification: _____

Person Conducting Certification _____

OPERATIONAL PROCEDURE REQUIRED BY PRIVACY AND SECURITY PLAN	A procedure is operational and:		No procedure is operational	Reason that procedure is not fully operational:				Estimated Date for procedure to be fully operational
	Procedure meets Plan requirements	Procedure does not meet Plan requirements		Cost constraints	Time constraints	Technological	Lack of authority	
4. Is there a procedure for an individual to challenge the accuracy of his or her CHRI?	_____	_____	_____	_____	_____	_____	_____	_____
5. Is there a process for administrative review and record correction?	_____	_____	_____	_____	_____	_____	_____	_____
6. Are appeal procedures clearly identified?	_____	_____	_____	_____	_____	_____	_____	_____
7. Are correction procedures clearly identified?	_____	_____	_____	_____	_____	_____	_____	_____
8. Is the information subject to review clearly identified?	_____	_____	_____	_____	_____	_____	_____	_____
9. Will procedures be operational by March 16, 1976 which allow an individual to access and review his or her CHRI?	_____	_____	_____	_____	_____	_____	_____	_____

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

Signed _____
(Head of Central Repository)

APPENDIX M

CRIMINAL JUSTICE SYSTEM STANDARDS AND GOALS

STANDARD 1.2: STATE ROLE IN CRIMINAL JUSTICE
INFORMATION AND STATISTICS

STANDARD

Utah should establish a criminal justice information system that provides the following services:

1. On-line files fulfilling a common need of all criminal justice agencies, including wanted persons (felony and misdemeanor), and identifiable stolen items;
2. Computerized criminal history files for all persons arrested, with an on-line availability of a summary of criminal activity and current status of offenders, and complete detailed criminal history files maintained on serious offenders in an off-line mode;
3. Access by computer interface to vehicle and driver files, if computerized and maintained separately by another State agency;
4. A high-speed interface with NCIC providing access to all NCIC files;
5. All necessary telecommunications media and terminals for providing access to local users, either by computer-to-computer interface or direct terminal access;
6. The computerized switching of agency-to-agency messages to and from qualified agencies in other States;
7. The collection, processing, and reporting of Uniform Crime Report (UCR) information from all law enforcement agencies in the State with report

generation for the Federal Government agencies, appropriate state agencies, and contributors;

8. In conjunction with criminal history files, the collection and storage of additional data elements and other features to support offender-based transaction statistics;

9. Entry and updating of data to a national index of criminal offenders as envisioned in the NCIC Computerized Criminal History file; and

10. Reporting offender-based transaction statistics to the Federal Government.

UTAH STATUS AND COMMENTS

Utah currently has an excess of 70,000 juvenile histories in an on-line status located in the central state computer. These files are currently used primarily by juvenile justice agencies; however, it is anticipated that certain data from these files will be made available to other criminal justice users. Computerized Criminal History files are currently available to criminal justice users on a limited basis. The Utah Computerized Criminal History files currently contain over 20,000 entries and include all offenses which a person may be arrested on as opposed to NCIC qualified offenses. The Computerized Criminal History file provides for on-line summary information with the complete history contained off-line on magnetic tape. Driver's License and Motor Vehicle files are currently available to all criminal justice users.

High speed interface to NCIC for the purpose of accessing files on the national level is currently in the development stage. A plan for providing

telecommunications media and terminals to allow access to local users is currently being implemented. Thirteen terminal sites are currently in operation with six additional sites to be installed during 1974. These sites involve a computer-to-computer interface between the state computer and the Salt Lake County computer and computer-to-terminal interface for all sites not serviced by the county computer. The capability of agency-to-agency administrative message switching is planned for but not implemented at this time. However, the capability to switch to other states from the Utah Bureau of Identification is currently available. The gathering of Uniform Crime Report information on a centralized level is currently under development in the state in conjunction with the Small Agency Record System (SARS). It is expected that this system will provide the basic data for the generation of UCR reports as well as other offense related statistical information.

Gathering of offender based transaction statistics is the task that is currently under development. Data elements to support the OBTS system will be collected in conjunction with the criminal history information. The entry and updating of criminal history information to the national index is currently being tested, and it is anticipated that this capability will be fully operational during 1974. The reporting of Offender Based Transaction Statistics information to the Federal government is under development with the expectation that initial testing will take place during 1974.

METHOD OF IMPLEMENTATION

This standard has been identified for implementation through administrative policy.

STANDARD 2.1: CRIMINAL JUSTICE AGENCY COLLECTION OF OBTS-CCH DATA

STANDARD

The collection of data required to satisfy both the OBTS and CCH systems should be gathered from operating criminal justice agencies in a single collection. Forms and procedures should be designed to assure that data coded by agency personnel meets all requirements of the information and statistics systems, and that no duplication of data is requested.

In order to maintain integrity in the data base and support from submitting agencies, it is imperative that appropriate procedures be generated on the state level to assure that all requirements for information are met.

UTAH STATUS AND COMMENTS

The Utah Criminal Justice Information System currently has designed and tested procedures which will generate data from the field to support the computerized criminal history data base in the arrest and judicial segments. Additional procedures will be established in 1974 that will provide for generating complete information from the correctional segment and will provide for the expanded OBTS data requirements.

METHOD OF IMPLEMENTATION

This standard has been identified for implementation through administrative policy.

STANDARD 2.2: OBTS-CCH FILE CREATION

STANDARD

Files created as data bases for OBTS and CCH systems, because of their common data elements and their common data input from operating agencies, should be developed simultaneously and maintained as much as possible within a single activity.

Juvenile record information should not be entered into adult criminal history files.

UTAH STATUS AND COMMENTS

The file creation for the Offender Based Transaction Statistics and Computerized Criminal History Systems are currently under development, the CCH file has been created and is in service at this time, and it is anticipated that during 1974 the OBTS file will be created for test purposes. Along with the creation of the OBTS file, it is projected that a common data base, which will feed both systems, will be generated. Juvenile record information currently exists in a separate file and is fully operational. Utah State Law prohibits the combining of adult criminal history and juvenile record information into one data base.

METHOD OF IMPLEMENTATION

This standard has been identified for implementation through administrative policy.

STANDARD 2.3: TRIGGERING OF DATA COLLECTION

STANDARD

With the exception of intelligence files, collection of criminal justice information concerning individuals should be triggered only by a formal event in the criminal justice process and contain only verifiable data. In any case where dissemination beyond the originating agency is possible, this standard should be inviolable.

UTAH STATUS AND COMMENTS

Currently it is the practice of the State of Utah to collect criminal justice information concerning individuals only after a formal event has occurred relative to the criminal justice process. Intelligence information contained in the computerized criminal history is all verifiable information. The source documents are maintained in hard copy or microfilm form.

METHOD OF IMPLEMENTATION

This standard has been identified for implementation through legislative action.

STANDARD 2.4: COMPLETENESS AND ACCURACY OF OFFENDER DATA

STANDARD

Agencies maintaining data or files on persons designated as offenders shall establish methods and procedures to insure the completeness and accuracy of data, including the following:

1. Every item of information should be checked for accuracy and completeness before entry into the system. In no event should inaccurate, unclear, incomplete, or ambiguous data be entered into a criminal justice information system. Data is incomplete, unclear, or ambiguous when it might mislead a reasonable person about the true nature of the information.

2. A system of verification and audit should be instituted. Files must be designated to exclude ambiguous or incomplete data elements. Steps must be taken during the acquisition process to verify all entries. Systematic audits must be conducted to insure that files have been regularly and accurately updated. Where files are found to be incomplete, all persons who have received misleading information should be immediately notified.

3. The following rules shall apply to purging these records:

- a. General file purging criteria. In addition to inaccurate, incomplete, misleading, unverified, and unverifiable items of information, information that, because of its age or for other reasons, is likely to be an

unreliable guide to the subject's present attitudes or behavior should be purged from the system. Files shall be reviewed periodically.

b. Purging by virtue of lapse of time. Every copy of criminal justice information concerning individuals convicted of a serious crime should be purged from active files 10 years after the date of release from supervision. In the case of less serious offenses the period should be 5 years. Information should be retained where the individual has been convicted of another criminal offense within the United States, where he is currently under indictment or the subject of an arrest warrant by a U. S. criminal justice agency.

c. Use of purged information. Information that is purged but not returned or destroyed should be held in confidence and should not be made available for review or dissemination by an individual or agency except as follows:

(1) Where necessary for in-house custodial activities of the record keeping agency or for the regulatory responsibilities of the Security and Privacy Council (Chapter 8);

(2) Where the information is to be used for statistical compilations or research studies, in which the individual's identity is not disclosed and from which it is not ascertainable;

(3) Where the individual to whom the information relates seeks to exercise rights of access and review of files pertaining to him;

(4) Where necessary to permit the adjudication of any claim by the individual to whom the information relates that it is misleading, inaccurate, or incomplete; or

(5) Where a statute of a State necessitates inquiry into criminal offender record information beyond the 5- and 10-year limitations.

When the information has been purged, and the individual involved subsequently wanted or arrested for a crime, such records should be re-opened only for purposes of subsequent investigation, prosecution, and disposition of that offense. If the arrest does not terminate in conviction, the records shall be reclosed. If conviction does result, the records should remain open and available.

Upon proper notice, a criminal justice agency should purge from its criminal justice information system all information about which a challenge has been upheld. Further, information should be purged by operation of statute, administrative regulation or ruling, or court decisions, or where the information has been purged from the files of the State which originated the information.

UTAH STATUS AND COMMENTS

In the existing computerized criminal history file all data which is entered into the system is first verified by coders to insure that the data is accurate and complete before entry into the system. In addition, computer edits are conducted to insure that data is entered properly and is reasonable as related to the transaction. System audits are provided to insure that all data scheduled for input to the computer actually was received on the automated file.

Currently records are maintained on the on-line summary file until the person is deceased or until the court orders the record to be expunged. Utah currently has no statute regarding the removal of criminal history information from an individual's file or regarding the removal of an individual's file from active status on the computer after a specific period of time has lapsed. State statute provides for individuals to have specific entries on their own record expunged via court order if those entries relate to an arrest that resulted in a non-conviction disposition.

METHOD OF IMPLEMENTATION

This standard has been identified for implementation through legislative action.

STANDARD 2.5: SEPARATION OF COMPUTERIZED FILES

STANDARD

For systems containing criminal offender data, the following protections should apply:

1. The portion of the computer used by the criminal justice systems should be under the management control of a criminal justice agency and should be dedicated in the following manner:

a. Files should be stored on the computer in such a manner that they cannot be modified, destroyed, accessed, changed, purged, or overlaid in any fashion by non-criminal-justice terminals.

b. The senior criminal justice agency employee in charge of computer operations should write and install, or cause to have written and installed, a program that will prohibit inquiry, record updates or destruction of records from any terminal other than criminal justice system terminals which are so designated.

The destruction of records should be limited to specifically designated terminals under the direct control of the criminal justice agency responsible for maintaining the files.

c. The senior criminal justice agency employee in charge of computer operations should have written and installed a classified program to detect and store for classified output all attempts to penetrate any criminal offender record information system, program, or file.

This program should be known only to the senior criminal justice agency, and the control employee and his immediate assistant, and the records of the program should be kept continuously under maximum security conditions. No other persons, including staff and repair personnel, should be permitted to know this program.

2. Under no circumstances should a criminal justice manual or computerized files be linked to or aggregated with non-criminal-justice files so as to provide centralized or direct access for the purpose of amassing information about a specified individual or specified group of individuals.

UTAH STATUS AND COMMENTS

Utah State statute directs that the division of Systems Planning and Computing will be responsible for maintaining computer files used by state agencies. The development of the Utah Criminal Justice Information System is being conducted under the Department of Public Safety in cooperation with the Systems Planning and Computing Division. All systems are developed by project personnel and computer support, and programming support is contracted with the Utah State Data Processing Center.

Currently, all files that are on the State of Utah computer as well as those files maintained on the Salt Lake County computer are designed such that non-criminal-justice users cannot access change, purge, or modify any record contained therein. Certain criminal justice data is restricted to specific criminal justice users as well. An example of this is the juvenile record which currently is accessed only by juvenile justice agencies. The

Utah Criminal Justice System currently does not have a classified program to detect and store for classified output all attempts to penetrate a criminal offender record by an unauthorized user. This provision will be added during 1974.

METHOD OF IMPLEMENTATION

This standard has been identified for implementation through legislative action.

STANDARD 2.6: ESTABLISHMENT OF COMPUTER INTERFACES FOR CRIMINAL JUSTICE INFORMATION SYSTEMS

STANDARD

The establishment of a computer interface to other criminal justice information systems will constitute the acceptance of responsibility for a control unit for those agencies served by the interface.

1. Each computer interface in the criminal justice hierarchy from local criminal justice information systems through the national systems will be considered a control terminal and allowed to interface if all of the identified responsibilities are accepted by that control unit.

2. Each control unit must maintain technical logging procedures and allow for 100 percent audit of all traffic handled by the interface. Criminal history response logs should be maintained for one year.

3. The control unit must maintain backup or duplicate copies of its files in secure locations away from the primary site.

4. All personnel involved in a system are subject to security checks.

5. The control unit must establish a log checking mechanism where machine-generated logs of other than "no record" responses are compared with manual terminal loss and discrepancies between the two resolved.

UTAH STATUS AND COMMENTS

The concept of the Utah Criminal Justice Information System terminal network is such that terminals in the system generally will serve more than

one jurisdiction. Even though less terminals will be ultimately installed under this concept, more users will be serviced by one terminal site. Currently, control for switching on the system is maintained at two sites, the Salt Lake County Computer Center and the Utah Data Processing Center. Logging of transactions is currently maintained on the state computer but not on the county computer; however, all shareable information system traffic passes through the state computer prior to being switched to the County Computer Center. The current configuration will be modified during 1974 to centralize all switching and control to one site. This site will provide for complete logging of all transactions and will maintain history information on these transactions.

METHOD OF IMPLEMENTATION

This standard has been identified for implementation through legislative action.

STANDARD 2.7: THE AVAILABILITY OF CRIMINAL JUSTICE INFORMATION SYSTEMS

STANDARD

The availability of the information system (the percentage of time when the system is fully operating and can process inquiries) should not be less than 90 percent. This availability must be measured at the device serving the user and may in fact be several times removed (technically) from the data base providing the information.

UTAH STATUS AND COMMENTS

Currently, the Utah Criminal Justice Information System provides information on those files which are on-line to criminal justice users on a 24-hour 7 day-a-week basis. The system currently functions on an excess of 90% availability to the user, and this includes scheduled down time for routine file maintenance.

METHOD OF IMPLEMENTATION

This standard has been identified for implementation through administrative policy.

STANDARD 3.2: PROGRAMING LANGUAGES

STANDARD

Every agency contemplating the implementation of computerized information systems should insure that specific programing language requirements are established prior to the initiation of any programing effort. The Utah Criminal Justice Information System coordination staff should provide the direction concerning programing language requirements already in force, or establish the requirements based on current or projected hardware and programing needs (especially from a system stand point) of present and potential users.

UTAH STATUS AND COMMENTS

Currently, the Utah Criminal Justice Information System development team prescribed specific program languages which are used in all modules. The existing standard is COBOL based languages; however, the freedom to select a specific language for a particular program must be maintained to insure speed and efficiency in all operating modules. Criminal Justice Information System modules tend to be very complex, and as a result, emphasis should be placed on efficiency rather than interstate compatibility when selecting computer languages.

METHOD OF IMPLEMENTATION

This standard has been identified for implementation through administrative policy.

The UCJIS telecommunications concept also provides for multiple agency servicing from one terminal site as opposed to updating individual terminals in each agency. This multiple agency concept will considerably increase the service available to each agency as well as reduce costs for operation of the system.

METHOD OF IMPLEMENTATION

This standard has been identified for implementation through administrative policy.

STANDARD 3.3: TELEPROCESSING

STANDARD

The Utah Criminal Justice Information System coordination staff should insure through a statewide criminal justice system telecommunications network that all agencies have contact with the central data bank via voice or computer terminal communications and that emphasis should be placed wherever possible on multiple agency telecommunication service centers. In the telecommunications design attention should be given to other criminal justice information systems (planned or in operation at the national, state, and local levels to insure the design includes provisions for interfacing with other systems as appropriate).

UTAH STATUS AND COMMENTS

The Utah Criminal Justice Information System is currently in the process of implementing statewide telecommunications capabilities in all segments of the criminal justice system. Currently, operating in parallel is the Utah Law Enforcement Teletype System which provides inter-agency communications between law enforcement agencies with the state and the Utah Bureau of Identification. After the Utah Criminal Justice Information System Telecommunications network is complete, all administrative message switching will be transferred to computer terminals, and the low speed teletype terminals will be removed from operation. This will, in effect, upgrade the administrative switching capabilities between agencies in the state as well as improve the speed of inter-state switching.

STANDARD 4.1: SECURITY AND PRIVACY ADMINISTRATION

STANDARD

1. State Enabling Act: The State of Utah should adopt enabling legislation for the protection of security and privacy in criminal justice information systems. The enabling statute shall establish an administrative structure, minimum standards for protection of security and privacy, and civil and criminal sanction for violation of statutes or rules and regulations adopted under it. This legislation should be designed to expand upon and enhance the existing Utah State statutes pertaining to the maintenance of Criminal Justice Information Systems data.

2. Security and Privacy Council: The State of Utah shall establish a privacy and security council. One-third of the members' named shall be private citizens who are unaffiliated with the State's criminal justice system. The remainder shall include representatives of the criminal justice system and other appropriate governmental agencies. The Privacy and Security Council shall be established to serve as a policy board on matters relating to security and privacy. Upon the advise and counsel of the board, the Commissioner will promulgate and enforce rules and regulations based on policy established by the Security and Privacy Council. Civil and criminal sanctions should be set forth in the enabling act for violation of the provision of the statutes or rules and regulations adopted under it. Penalty should apply to improper collection, storage, access, and dissemination of criminal justic information.

3. Training of System Personnel and Public Education: Provisions for training persons involved in the direct operation of a criminal justice information system, regarding the proper use and control of the system, should be provided by appropriate criminal justice agencies. The curriculum, materials, and instructors' qualifications for any course of instruction regarding the use and control of the system should be approved by the Council.

UTAH STATUS AND COMMENTS

Legislation has been enacted in the State of Utah which provides for limiting access and the dissemination of criminal history information. The statute identifies as a misdemeanor, punishable by fine and/or sentencing to the county jail, the unauthorized dissemination of criminal history information. The statute primarily relates to the security of the system as opposed to providing safeguards for the individual privacy of information. The Utah statute authorizes the Commissioner of Public Safety to enforce and administer the provisions of the statute through the Utah Bureau of Criminal Identification. Utah currently does not have a privacy and security council due to the provision in the statute that designates the Commissioner of Public Safety to enforce the provisions of the statute. Penalties for the improper collection or storage of criminal history data do not exist under the current statute. However, the Commissioner of Public Safety is authorized to develop and enforce the necessary safeguards to the system. Utah does not currently have a formalized system for the training of systems personnel or an organized method of providing public education.

Systems training regarding the operation of the criminal justice information system and its proper use and control, are provided on an as needed basis by the appropriate jurisdiction. Enabling legislation regarding privacy and security of criminal justice information systems has been enacted in several states with varying degrees of restrictiveness regarding the type of information maintained. The most workable configuration noted thus far uses general enabling legislation, which essentially is not self-executing, in conjunction with an administrative body which has the responsibility to oversee the protection of security and privacy. In most states with enabling legislation, the administrative body is charged with generating administrative policies and procedures, and with the enforcement of the same.

The trend toward enabling legislation with an administrative body to execute the responsibilities of the act is the result of the complexed and dynamic nature of criminal justice information systems.

METHOD OF IMPLEMENTATION

This standard has been identified for implementation through legislative action.

STANDARD 4.2: SCOPE OF FILES

STANDARD

In determining whether data should be collected and stored, the criminal justice submitting agency should take into consideration the potential benefits of the information against the potential injury to privacy and related protective interests.

UTAH STATUS AND COMMENTS

Criminal justice agencies in the State of Utah have restricted themselves primarily to the use of data pertinent to their activities. This is partially expressed in the state's statutes and additionally through administrative practice as defined on the agency level. The formalizing of policy for systemized application weighing potential injury to privacy as related to potential benefits to the system does not exist.

METHOD OF IMPLEMENTATION

This standard has been identified for implementation through administrative policy.

STANDARD 4.3: ACCESS AND DISSEMINATION

STANDARD

1. General Limits on Access. Information in criminal justice files should be made available only to public agencies which have both a "need to know" and a "right to know." The user agency should demonstrate, in advance, that access to such information will serve a criminal justice purpose.

2. Terminal Access. Criminal justice agencies should be permitted to have terminal access to computerized criminal justice information systems where they have both a need and a right to know. Non-criminal justice agencies having a need or right to know or being authorized by statute to receive criminal justice information should be supplied with such information only through criminal justice agencies.

3. Certification of Non-Criminal-Justice Users. The Commissioner of Public Safety should receive and review applications from non-criminal-justice government agencies for access to criminal justice information. Each agency which has, by statute, a right to such information or demonstrates a need to know and a right to know in furtherance of a criminal justice purpose should be certified as having access to such information through a designated criminal justice agency.

4. Full and Limited Access to Data. Criminal justice agencies should be entitled to all unpurged data concerning an individual contained in a crimi-

nal justice information system. Non-criminal-justice agencies should receive only those portions of the file directly related to the inquiry. Special precautions should be taken to control dissemination to non-criminal-justice agencies of information which might compromise personal privacy including strict enforcement of need to know and right to know criteria.

5. Arrest without Conviction. All copies of information filed as a result of an arrest that is legally terminated in favor of the arrested individual should be returned to that individual within 60 days of final disposition, if a court order is presented, or upon formal notice from one criminal justice agency to another. Information includes fingerprints and photographs. Such information should not be disseminated outside criminal justice agencies.

However, files may be retained if another criminal action or proceeding is pending against the arrested individual, or if he has previously been convicted in any jurisdiction in the United States of an offense that would be deemed a crime in the State of Utah.

6. Dissemination. Dissemination of personal criminal justice information should be on a need and right to know basis within the government. There should be neither direct nor indirect dissemination of such information to non-governmental agencies or personnel. Each receiving agency should restrict internal dissemination to those employees with both a need and right to know.

Legislation should be enacted which limits questions about arrests on applications for employment, licenses, and other civil rights and privileges

to those arrests where records have not been returned to the arrested individual or purged. Nor shall employers be entitled to know about offenses that have been expunged by virtue of lapse of time (see Standard 2.4).

7. Accountability for Receipt, Use, and Dissemination of Data. Each person and agency that obtains access to criminal justice information should be subject to civil, criminal, and administrative penalties for the improper receipt, use, and dissemination of such information.

The penalties imposed would be those generally applicable to breaches of system rules and regulations as noted earlier.

8. Currency of Information. Each criminal justice agency must ensure that the most current record is used or obtained.

UTAH STATUS AND COMMENTS

Utah State Statute currently limits access to criminal history information as opposed to criminal justice information and provides the Commissioner of Public Safety with the authority to administratively set policies regarding the dissemination of this data. The access to data, via computer terminals, is currently limited by policy established by the Utah Bureau of Identification. Currently, a statute outlining agencies having a need or right to criminal justice information does not exist.

The certification of non-criminal-justice users to receive information from other than remote terminals is provided by statute through the Commissioner of Public Safety. Utah State Statute allows the Commissioner of Public Safety to determine which non-criminal justice agencies should

receive criminal history information. There is currently no provision to restrict portions of a criminal history record to authorized non-criminal justice agency users. In practice, if an agency is authorized to access the criminal history file, the contents of the entire rap sheet are made available. The expungement, or sealing of criminal history records, currently can only be done as a result of a court order. Expungement generally relates to a specific entry on the record as opposed to the entire record. One problem that has been encountered in orders to expunge is the lack of specific detail entered onto the order by the court which results in unclear instructions.

If the court finds that the petitioner, for a period of five years in the case of an indictable misdemeanor or felony, or for a period of three years in the case of a misdemeanor, since his release from incarceration or probation, has not been convicted of a felony or of a misdemeanor involving moral turpitude and that no proceeding involving such a crime is pending or being instituted against the petitioner and, further, finds that the rehabilitation of the petitioner has been attained to the satisfaction of the court, it shall enter an order that all records in the petitioner's case in the custody of that court or in the custody of any other court agency or official, be sealed.

The dissemination of the personal criminal history information is based on a need and right to know basis with the Commissioner of Public Safety charged with the responsibility of determining which agencies should receive information. Currently, penalties exist for the improper use and dissemination of criminal history data.

METHOD OF IMPLEMENTATION

This standard has been identified for implementation through administrative police except in those provisions indicating legislative action.

STANDARD 4.4: INFORMATION REVIEW

STANDARD

1. Right to Review Information. Except for intelligence files, every person should have the right to review criminal justice information relating to him. Each criminal justice agency with custody or control of criminal justice information shall make available convenient facilities and personnel necessary to permit such reviews.

2. Review Procedures.

a. Reviews should occur only within the facilities of a criminal justice agency and only under the supervision and in the presence of a designated employee or agent of a criminal justice agency. The files and records made available to the individual should not be removed from the premises of the criminal justice agency at which the records are being reviewed.

b. At the discretion of each criminal justice agency such reviews may be limited to ordinary daylight business hours.

c. Reviews should be permitted only after verification that the requesting individual is the subject of the criminal justice information which he seeks to review. Each criminal justice agency should require fingerprinting for this purpose. Upon presentation of a sworn authorization from the individual involved, together with proof of identity, an individual's attorney may be permitted to examine the information relating to such individual.

d. A record of such review should be maintained by each criminal justice agency by the completion and preservation of an appropriate form. Each form should be completed and signed by the supervisory employee or agent present at the review. The reviewing individual should be asked, but may not be required, to verify by his signature the accuracy of the criminal justice information he has reviewed. The form should include a recording of the name of the reviewing individual, the date of the review, and whether or not any exception was taken to the accuracy, completeness, or contents of the information reviewed.

e. The reviewing individual may make a written summary or notes in his own handwriting of the information reviewed, and may take with him such copies. Such individuals may not, however, take any copy that might reasonably be confused with the original. Criminal justice agencies are not required to provide equipment for copying.

f. Each reviewing individual should be informed of his rights of challenge. He should be informed that he may submit written exceptions as to the information's contents, completeness or accuracy to the criminal justice agency with custody or control of the information. Should the individual elect to submit such exceptions, he should be furnished with an appropriate form. The individual should record any such exceptions on the form. The form should include an affirmation, signed by the individual or his legal representative, that the exceptions are made in good faith

that they are true to the best of the individual's knowledge and belief.

One copy of the form shall be forwarded to the Commissioner of Public Safety.

g. The criminal justice agency should in each case conduct an audit of the individual's criminal justice information to determine the accuracy of the exceptions. The Commissioner of Public Safety and the individual should be informed in writing of the results of the audit. Should the audit disclose inaccuracies or omissions in the information, the criminal justice agency should cause appropriate alterations or additions to be given to the Commissioner of Public Safety, the individual involved, and any other agencies in this or any other jurisdiction to which the criminal justice information has previously been disseminated.

3. Challenges to Information.

a. Any person who believes that criminal justice information that refers to him is inaccurate, incomplete, or misleading may request any criminal justice agency with custody or control of the information to purge, delete, modify, or supplement that information. Should the agency decline to do so, or should the individual believe the agency's decision to be otherwise unsatisfactory, the individual may request review by the Commissioner of Public Safety.

b. Such requests to the Commissioner of Public Safety (in writing) should include a concise statement of the alleged deficiencies of the criminal justice information, shall state the date and result of any review by

the criminal justice agency, and shall append a sworn verification of the facts alleged in the request signed by the individual or his attorney.

c. The Commissioner of Public Safety should establish a review procedure for such appeals that incorporate appropriate assurances of due process for the individual.

UTAH STATUS AND COMMENTS

Currently in the State of Utah, a person may view his own criminal history information event, though this is not specifically outlined in the state statutes. When reviews are permitted, they are performed within the facilities of a criminal justice agency under supervision, and the files are not allowed to leave the premises. Generally, records of such a review are not maintained, and the reviewing of the individual is not required to verify the accuracy of the information that he has reviewed. Specific audit procedures have not been established to determine the accuracy of any exceptions an individual may take; however, complete audits are performed on the data in question if challenges are made.

METHOD OF IMPLEMENTATION

This standard has been identified for implementation through legislative action.

STANDARD 4.5: DATA SENSITIVITY CLASSIFICATION

STANDARD

The Security and Privacy Council may classify information in criminal justice information systems in accordance with the following system:

1. Highly Sensitive - places and things which require maximum special security provisions and particularized privacy protection. Items that should be included in this category include, for example:

a. Criminal history record information accessed by using other than personal identifying characteristics, i. e., class access;

b. Criminal justice information disclosing arrest information without conviction disseminated to criminal justice agencies;

c. Criminal justice information marked as "closed";

d. Computer, primary, and auxiliary storage devices and physical contents, peripheral hardware, and certain manual storage devices and physical contents;

e. Security system and backup devices; and

f. Intelligence files.

g. Additional items that may be included in this category are: computer programs and system design; communication devices and networks; criminal justice information disseminated to non-criminal-justice agencies; and research and analytical reports derived from identified individual criminal justice information.

2. Confidential - places and things which require a high degree of special security and privacy protection. Items that may be included in this category, for example, are:

- a. Criminal justice information on individuals disseminated to criminal justice agencies;
- b. Documentation concerning the system; and
- c. Research and analytical reports derived from criminal justice information on individuals.

3. Restricted - places and things which require minimum special security consistent with good security and privacy practices. Places that may be included in this category are, for example, areas and spaces that house criminal justice information.

Each criminal justice agency maintaining criminal justice information should establish procedures in order to implement a sensitivity classification system. The general guidelines for this purpose are:

- a. Places and things should be assigned the lowest classification consistent with their proper protection.
- b. Appropriate utilization of classified places and things by qualified users should be encouraged.
- c. Whenever the sensitivity of places or things diminishes or increases, it should be reclassified without delay.
- d. In the event that any place or thing previously classified is no longer sensitive and no longer requires special security or privacy protection, it should be declassified.

e. The originator of the classification is wholly responsible for reclassification and declassification.

f. Overclassification should be considered to be as dysfunctional as underclassification.

It shall be the responsibility of the Commissioner of Public Safety to assure that appropriate classification systems are implemented, maintained, and complied with by criminal justice agencies within a given state.

UTAH STATUS AND COMMENTS

Utah currently does not have a data sensitivity classification system for places and things, including data which is part of the criminal justice information system. The system currently used in Utah is primarily centered around the concept that all data, places, and things are sensitive, and procedures have been developed to assist in providing adequate security.

Even though procedures have been developed, the most stringent in existence in the state would not meet the category outlined in Standard 8.5 as being classified "highly sensitive." Procedures currently used throughout the state would be placed in the confidential and restricted categories for the most part, even though no specific attempt is made to classify places or things at the present time. Existing procedures and safeguards are not adequate due to a variety of weakpoints throughout the system. The most glaring example of weakness in the physical security area is the row of windows on the north side of the Utah State Data Processing Center computer facility, which would provide access, via a variety of projectiles, to the computer and adjacent disc files.

CONTINUED

3 OF 4

METHOD OF IMPLEMENTATION

This standard has been identified for implementation through administrative policy.

STANDARD 4.6: SYSTEM SECURITY

STANDARD

1. Protection from Accidental Loss. Information system operators should institute procedures for protection of information from environmental hazards including fire, flood, and power failure. Appropriate elements should include:

- a. Adequate fire detection and quenching systems;
- b. Watertight facilities;
- c. Protection against water and smoke damage;
- d. Liaison with local fire and public safety officials;
- e. Fire resistant materials on walls and floors;
- f. Air conditioning systems;
- g. Emergency power sources; and
- h. Backup files.

2. Intentional Damage to System. Agencies administering criminal justice information systems should adopt security procedures which limit access to information files. These procedures should include use of guards, keys, badges, passwords, access restrictions, sign-in logs, or like controls.

All facilities which house criminal justice information files should be so designed and constructed as to reduce the possibility of physical damage to the information. Appropriate steps in this regard include: physical limitations on access; security storage for information media; heavy duty, non-exposed

walls; perimeter barriers; adequate lighting; detection and warning devices, and closed circuit television.

3. Unauthorized Access. Criminal justice information systems should maintain controls over access to information by requiring identification, authorization, and authentication of system users and their need and right to know. Processing restrictions, threat monitoring, privacy transformations (e.g., scrambling, encoding/decoding), and integrity management should be employed to ensure system security.

4. Personnel Security.

a. Preemployment Screening: Applicants for employment in information systems should be expected to consent to an investigation of their character, habits, previous employment, and other matters necessary to establish their good moral character, reputation, and honesty. Giving false information of a substantial nature should disqualify an applicant from employment.

Investigation should be designed to develop sufficient information to enable the appropriate officials to determine employability and fitness of persons entering critical/sensitive positions. Whenever practical, investigations should be conducted on a preemployment basis and the resulting reports used as a personnel selection device.

b. Clearance, Annual Review, Security Manual, and In-Service Training: System personnel including terminal operators in remote locations, as well as programmers, computer operators, and others working

at, or near the central processor, should be assigned appropriate security clearances renewed annually after investigation and review.

The Utah Criminal Justice Information System staff should prepare a security manual listing the rules and regulations applicable to maintenance of systems security. Each person working with or having access to criminal justice information files should know the contents of the manual.

c. System Discipline: The management of each criminal justice information system should establish sanctions for accidental or intentional violation of system security standards. Supervisory personnel should be delegated adequate authority and responsibility to enforce the system's security standards.

Any violations of the provisions of these standards by any employee or officer of any public agency, in addition to any applicable criminal or civil penalties, shall be punished by suspension, discharge, reduction in grade, transfer, or such other administrative penalties as are deemed by the criminal justice agency to be appropriate.

Where any public agency is found by the Commissioner of Public Safety willfully or repeatedly to have violated the requirements of the standard (act), the Commissioner of Public Safety may, where other statutory provisions permit, prohibit the dissemination of criminal history record information to that agency, for such periods and on such conditions as the Commissioner of Public Safety deems appropriate.

UTAH STATUS AND COMMENTS

Utah Criminal Justice Information System files are all designed and maintained with off-line backup. As on-line files are updated, update transactions are written on magnetic tapes where they are stored in another location. The procedures used on all UCJIS files allow for data loss only during the time between machine encoding and the system update, which generally is a 24-hour period. In the event that data is lost during this time, paper files are maintained as backup, in the event that machine encoding would have to be repeated.

All locations currently housing automated files are adequately protected from potential fire damage. Air conditioning systems are part of each installation, but the lack of emergency backup power sources is a major weakness in the system. Backup power generators, in the event of primary source power failure, are extremely expensive and as a result, have not been installed.

The access to physical computer facilities is controlled by using name badges and double locking doors at the state computer center. During evening hours, building security is increased by the use of guards and sign-in logs. The major weakness in guarding against physical damage is the inadequate security of walls surrounding the area which contains the computer.

Currently, the electronic access from remote locations is limited to specific users which are identified electronically prior to sending a message or receiving an inquiry. In this manner, information from specific

files can be released to specific predetermined users only. An example of this currently is with the limited access of juvenile history information, which is available only to juvenile justice agencies throughout the state.

Personnel security is currently maintained through pre-employment screening by the Utah Bureau of Identification. All personnel who currently are employed and have access to a portion of the system have also been cleared. Once a person has been screened, the clearance remains good until he terminates employment or violates system security. Annual reviews are not conducted, and scheduled in-service training is not required or provided.

METHOD OF IMPLEMENTATION

This standard has been identified for implementation through legislative action.



STANDARD 4.7: PERSONNEL CLEARANCES

STANDARD

1. The Commissioner of Public Safety may also have the responsibility of assuring that a personnel clearance system is implemented and complied with by criminal justice agencies within the State.

2. Personnel may be granted clearances for access to sensitive places and things in accordance with strict right to know and need to know principles.

3. In no event may any person who does not possess a valid sensitivity clearance indicating right to know have access to any classified places or things, and in no event may any person have access to places or things of a higher sensitivity classification than the highest valid clearance held by that person.

4. The possession of a valid clearance indicating right to know does not warrant unconditional access to all places and things of the sensitivity classification for which the person holds clearance. In appropriate cases such persons may be denied access because of absence of need to know.

5. In appropriate cases, all persons in a certain category may be granted blanket right to know clearance for access to places and things classified as restricted or confidential.

6. Right to know clearances for highly sensitive places and things may be granted on a selective and individual basis only and must be based upon the strictest of personnel investigations.

7. Clearances may be granted by the head of the agency concerned and may be binding only upon the criminal justice agency itself.

8. Clearances granted by one agency may be given full faith and credit by another agency; however, ultimate responsibility for the integrity of the persons granted right to know clearances remains at all times with the agency granting the clearance.

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

10. It may be the responsibility of the criminal justice agency with custody and control of classified places and things to prevent compromise of such places and things by prohibiting access to persons without clearances or with inadequate clearance status.

11. The Commissioner of Public Safety may carefully audit the granting of clearances to assure that they are valid in all respects, and that the categories of personnel clearances are consistent with right to know and need to know criteria.

12. Criminal justice agencies may be cognizant at all times of the need periodically to review personnel clearances so as to be certain that the lowest possible clearance is accorded consistent with the individual's responsibilities.

13. To provide evidence of a person's sensitivity classification clearance, the grantor of such clearance may provide an authenticated card or certificate. Responsibility for control of the issuance, adjustment, or revocation of such documents must have an automatic expiration date requiring affirmative renewal after a reasonable period of time.

UTAH STATUS AND COMMENTS

Currently, the Utah Bureau of Identification screens employees who will have contact with files contained in the Utah Criminal Justice Information System. However, specific security clearance classifications are not assigned. All persons cleared are considered to have equal status. The access of specific data, however, is restricted to specific individuals as is related to their need to know. For example, persons cleared for accessing data for research as in the Utah Criminal Justice Information Systems Data Center would not be authorized to perform name checks on persons listed on the criminal history file without prior approval from the director of the bureau.

User agencies are held responsible for the clearing of all persons using the system on that level; however, no specific procedures have been established nor checks performed to insure that this is the case. Individual

criminal justice agencies have developed internal policies for the screening of personnel, and even though these procedures vary from agency to agency, screening does occur. Even though specific clearance is not issued, representatives from one agency are generally recognized by another agency for the purpose of accessing criminal justice information.

METHOD OF IMPLEMENTATION

This standard has been identified for implementation through administrative policy.

STANDARD 4.8: INFORMATION FOR RESEARCH

STANDARD

1. Research Design and Access to Information. Researchers who wish to use criminal justice information should submit to the agency holding the information a complete research design that guarantees adequate protection of security and privacy. The design as well as the output should be approved by the agency responsible for disseminating the information prior to the conducting of the study. Persons conducting research should all have appropriate security clearances before being allowed file access.

2. Limits on Criminal Justice Research. Research should preserve the anonymity of all subjects to the maximum extent possible. All data released by the research effort shall contain no information that would identify any subject used in the study. All raw data used in the study shall be returned to the custody of the holding agency at the conclusions of the research effort. In no case should criminal justice research be used to the detriment of persons to whom information relates nor for any purposes other than those specified in the research proposal. Each person having access to criminal justice information should execute a binding nondisclosure agreement, with penalties for violation.

3. Role of Privacy and Security Council. The Privacy and Security Council should establish uniform criteria for protection of security and pri-

vacy in research programs. If a research or an agency is in doubt about the security or privacy aspects of a particular research project or activities, the advice of the Commissioner of Public Safety should be sought.

4. Duties and Responsibilities of the Holding Agency. Criminal justice agencies should retain and exercise the authority to approve in advance, monitor, and audit all research using criminal justice information. All data gathered by the research program should be examined and verified. Data should not be released for any purposes if material errors or emissions have occurred which would effect security and privacy.

UTAH STATUS AND COMMENTS

Currently, the Utah Criminal Justice Information Systems Data Center performs research using information from computerized as well as manual files. Operating procedures have been established in this unit to insure that all research utilizing offender data be done without any cross reference to data elements which would identify the individuals under study. In addition, specific procedures have been established to insure that data is released only with specific approval of the Utah Criminal Justice Information Systems Coordinator and the Director of the Utah Law Enforcement Planning Agency.

In performing research it may be necessary to utilize specific identifiers which could lead to the identification of an individual; however, the major point of concern is the form the data is in when it is released beyond the research staff. Currently, other requests for statistical information, such as through the Utah Bureau of Identification, are released without specific data that would identify individuals that were used in generating the data.

METHOD OF IMPLEMENTATION

This standard has been identified for implementation through administrative policy.

STANDARD 8.1: LEGISLATIVE ACTIONS

STANDARD

To provide a solid basis for the development of systems supporting criminal justice, at least three legislative actions are needed:

1. Statutory authority should be established for planning, developing, and operating State level information and statistical systems.
2. Utah should establish, by statute, taking into consideration the proper relationship of the three branches of government, mandatory reporting of data necessary to operate the authorized system.
3. Statutes should be enacted to establish security and confidentiality controls on all systems.

UTAH STATUS AND COMMENTS

Currently, mandatory reporting legislation for criminal justice agencies does exist with the Commissioner of Public Safety through the Utah Bureau of Identification (UBI) charged with the maintenance and dissemination of criminal justice information. The statute, however, deals only with offender records and other information related specifically to the police segment of the criminal justice system.

Currently, statutes related to maintaining security and confidentiality controls on all systems throughout the state do not exist, even though existing state statutes do refer to the control of criminal history information at the state level.

METHOD OF IMPLEMENTATION

This standard has been identified for implementation through legislative action.

APPENDIX N

STATE CENTRAL REPOSITORY
CERTIFICATION CHECKLIST

CERTIFICATION FORM/PROCESS NO. (1, 2, 3, 4, 5, CENTRAL REPOSITORY)

AGENCY: UTAH STATE BUREAU OF CRIMINAL IDENTIFICATIONDate of Certification: JANUARY 20, 1976SALT LAKE CITY, UTAH 84114Person Conducting Certification RICHARD HORLACHER

OPERATIONAL PROCEDURE REQUIRED BY PRIVACY AND SECURITY PLAN	A procedure is operational and:		Reason that procedure is not fully operational:				Estimated date for procedure to be fully operational
	Procedure meets Plan requirements	Procedure does not meet Plan requirements	Cost constraints	Time constraints	Technological	Lack of authority	
A. Completeness and Accuracy Procedures							
1. Is there a State or local agency Central Repository?	X						
a. Is there Statutory/Executive authority for the Central Repository?	X						
b. Are facilities and staff adequate to provide CHRI services Statewide or locally?			X	X	X		12/77
2. Is there a disposition reporting system?			X		X		12/76
a. Is disposition reporting provided within 90 days from:							
1. Police			X		X		12/77
2. Prosecutors			X		X		12/77
3. Trial Courts			X		X		12/77
4. Appellate Courts			X		X		12/77
5. Correctional Institutions			X		X		12/77
6. Probation and Parole Agencies			X		X		12/77

PROCESS NO. (1, 2, 3, 4, 5, CENTRAL REPOSITORY)

AGENCY: UTAH STATE BUREAU OF CRIMINAL IDENTIFICATIONDate of Certification: JANUARY 20, 1976SALT LAKE CITY, UTAH 84114Person Conducting Certification RICHARD MORLACHER

OPERATIONAL PROCEDURE REQUIRED BY PRIVACY AND SECURITY PLAN	A procedure is operational and:		Reason that procedure is not fully operational:				Estimated date for procedure to be fully operational	
	Procedure meets Plan requirements	Procedure does not meet Plan requirements	No procedure is operational	Cost constraints	Time constraints	Technological	Lack of authority	
b. Is there a Delinquent Disposition Monitoring System to provide for:								
1. Delinquent disposition monitoring			X			X		12/77
2. One-year rule/dissemination without disposition			X			X		12/77
3. Terminal output flags			X			X		12/77
c. Is there a procedure to report disposition of arrests occurring after June 19, 1975 within the 90-day rule?			X			X		12/77
3. Are there procedures for repository query by criminal justice agencies before CHRI dissemination?			X			X		12/77
a. Are query requirements documented?			X			X		12/77
b. Are written agreements with user agencies in existence?			X			X		12/77
4. Are there procedures to maintain accuracy of records?	X							
a. Is notification on inaccurate information provided?			X			X		12/77

PROCESS NO. (1, 2, 3, 4, 5, CENTRAL REPOSITORY)

AGENCY: UTAH STATE BUREAU OF CRIMINAL IDENTIFICATIONDate of Certification: JANUARY 20, 1976SALT LAKE CITY, UTAH 84114Person Conducting Certification RICHARD HOBLACHER

OPERATIONAL PROCEDURE REQUIRED BY PRIVACY AND SECURITY PLAN	A procedure is operational and:		Reason that procedure is not fully operational:				Estimated date for procedure to be fully operational
	Procedure meets Plan requirements	Procedure does not meet Plan requirements	Cost constraints	Time constraints	Technological	Lack of authority	
5. Are CHRI dissemination and manual file screening procedures in use with criminal history record systems other than the Central Repository (UBI)?			X		X		12/77
B. <u>Limits on Dissemination Procedures</u>							
1. Are general policies on use and dissemination documented?	X						
and							
Are there procedures restricting and limiting dissemination in the following situations:							
a. Juvenile record dissemination	N/A						
b. Confirmation of record existence		X			X		
c. Secondary dissemination by non-criminal justice agencies			X				
2. Are there sanctions for individuals and agencies authorized who violate CHRI dissemination policies?	X						

Date of Certification: JANUARY 20, 1976

Person Conducting Certification RICHARD HORLACHER

OPERATIONAL PROCEDURE REQUIRED BY PRIVACY AND SECURITY PLAN		A procedure is operational and:		Reason that procedure is not fully operational:				Estimated date for procedure to be fully operational	
		Procedure meets Plan requirements	Procedure does not meet Plan requirements	No procedure is operational	Cost constraints	Time constraints	Technological		Lack of authority
3. Are there procedures for validating agency right of access for:									
a. Criminal justice agencies		X							
b. Non-criminal justice agencies			X						
c. Service agencies under contract			X						
d. Research organizations			X						
e. Right of access validation			X						
4. Are notices presented to agencies not directly subject to the regulations?				X			X		12/77
C. <u>Audits and Quality Control Procedures</u>									
1. Is there a systematic audit (quality controls) process providing:									
a. Audit trails			X						12/77
b. Accuracy checks		X							12/77
c. Random document and record inspection		X							12/77
d. Dissemination logs				X			X		12/77
2. Are annual audits/compliance reviews performed on:									
a. Central Repository (UBI)									

AGENCY: UTAH STATE BUREAU OF CRIMINAL IDENTIFICATIONDate of Certification: JANUARY 20, 1976SALT LAKE CITY, UTAH 84114Person Conducting Certification RICHARD HORLACHER

OPERATIONAL PROCEDURE REQUIRED BY PRIVACY AND SECURITY PLAN	A procedure is operational and:			Reason that procedure is not fully operational:				Estimated date for procedure to be fully operational
	Procedure meets Plan requirements	Procedure does not meet Plan requirements	No procedure is operational	Cost constraints	Time constraints	Technological	Lack of authority	
b. Other state and local systems			X	X	X	X		12/77
c. Documents and data to be maintained			X	X	X	X		
D. Security and Confidentiality Procedures								
I. Does the hardware and software provide for:								
a. General security provisions	X							
b. Procedures for access	X							
c. Dedication of:								
1. Terminals	X							
2. Communications control		X						
3. Processor		X						
4. Storage devices		X						
and does the software provide maximum security of CHRI?	X							
2. Is there adequate management control and is a responsible agency designated to provide for:								
a. Management control and accountability	X							

PROCESS NO. (1, 2, 3, 4, 5, CENTRAL REPOSITORY)

AGENCY: UTAH STATE BUREAU OF CRIMINAL IDENTIFICATIONDate of Certification: JANUARY 20, 1976SALT LAKE CITY, UTAH 84114Person Conducting Certification RICHARD HORLACHER

OPERATIONAL PROCEDURE REQUIRED BY PRIVACY AND SECURITY PLAN	A procedure is operational and:		Reason that procedure is not fully operational:				Estimated date for procedure to be fully operational	
	Procedure meets Plan requirements	Procedure does not meet Plan requirements	No procedure is operational	Cost constraints	Time constraints	Technological	Lack of authority	
b. Computer operations policy		X						
c. Access to criminal history records	X							
d. Sanctions for misuse	X							
3. Does the personnel process provide:								
a. Selection and security screening	X							
b. Supervision			X			X		
c. Training			X			X		
4. Is there physical security to:								
a. Protect against environmental hazards	X							
b. Prevent physical access by unauthorized personnel	X							
c. Secure facilities construction	X							

PROCESS NO. (1, 2, 3, 4, 5, CENTRAL REPOSITORY)

AGENCY: UTAH STATE BUREAU OF CRIMINAL IDENTIFICATIONDate of Certification: JANUARY 20, 1976SALT LAKE CITY, UTAH 84114Person Conducting Certification RICHARD HORLACHER

OPERATIONAL PROCEDURE REQUIRED BY PRIVACY AND SECURITY PLAN	A procedure is operational and:		No procedure is operational	Reason that procedure is not fully operational:				Estimated date for procedure to be fully operational
	Procedure meets Plan requirements	Procedure does not meet Plan requirements		Cost constraints	Time constraints	Technological	Lack of authority	
E. <u>Individual Right of Access Procedures</u>								
1. Are there adequate procedures to verify identity before releasing information?	_____	_____	<u>X</u>	_____	_____	_____	<u>X</u>	<u>3/76</u>
2. Are the rules for access written and disseminated to the public?	_____	_____	<u>X</u>	_____	_____	_____	<u>X</u>	<u>3/76</u>
3. Is there a specified and convenient point of review and mechanism for review of CHRI?	_____	_____	<u>X</u>	_____	_____	_____	<u>X</u>	<u>3/76</u>

PROCESS NO. (1, 2, 3, 4, 5, CENTRAL REPOSITORY)

AGENCY: UTAH STATE BUREAU OF CRIMINAL IDENTIFICATIONDate of Certification: JANUARY 20, 1976SALT LAKE CITY, UTAH 84114Person Conducting Certification Richard Horlacher

OPERATIONAL PROCEDURE REQUIRED BY PRIVACY AND SECURITY PLAN	A procedure is operational and:		No procedure is operational	Reason that procedure is not fully operational:				Estimated date for procedure to be fully operational
	Procedure meets Plan requirements	Procedure does not meet Plan requirements		Cost constraints	Time constraints	Technological	Lack of authority	
4. Is there a procedure for an individual to challenge the accuracy of his or her CHRI?			X				X	3/76
5. Is there a process for administrative review and record correction?			X				X	3/76
6. Are appeal procedures clearly identified?			X				X	3/76
7. Are correction procedures clearly identified?			X				X	3/76
8. Is the information subject to review clearly identified?			X				X	3/76
9. Will procedures be operational by March 16, 1976 which allow an individual to access and review his or her CHRI?			X				X	3/76

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

Signed David R. Rogers

(Head of Central Repository)

APPENDIX O

CERTIFICATION CHECKLISTS FOR OTHER AGENCIES

The certification forms for the criminal justice agencies who were certified are on file with the Department of Public Safety. Copies of these forms were included in the copies of the Plan which were submitted to LEAA.

Date of Certification: _____

OPERATIONAL PROCEDURE REQUIRED
BY PRIVACY AND SECURITY PLAN

A procedure is operational and:

No procedure is operational

Reason that procedure
is not fully operational:

Procedure meets Plan requirements

Procedure does not meet Plan requirements

Cost constraints

Time constraints

Technological

Lack of authority

Estimated date
for procedure to be
fully operational

A. Completeness and Accuracy Procedures

1. Is there a State or local agency Central Repository?
 - a. Is there Statutory/Executive authority for the Central Repository?
 - b. Are facilities and staff adequate to provide CHRI services Statewide or locally?
2. Is there a disposition reporting system?
 - a. Is disposition reporting provided within 90 days from:
 1. Police
 2. Prosecutors
 3. Trial Courts
 4. Appellate Courts
 5. Correctional Institutions
 6. Probation and Parole Agencies

Date of Certification: _____

OPERATIONAL PROCEDURE REQUIRED
BY PRIVACY AND SECURITY PLAN

OPERATIONAL PROCEDURE REQUIRED BY PRIVACY AND SECURITY PLAN	A procedure is operational and:		No procedure is operational	Reason that procedure is not fully operational:				Estimated date for procedure to be fully operational
	Procedure meets Plan requirements	Procedure does not meet Plan requirements		Cost constraints	Time constraints	Technological	Lack of authority	
b. Is there a Delinquent Disposition Monitoring System to provide for: 1. Delinquent disposition monitoring 2. One-year rule/dissemination without disposition 3. Terminal output flags	 	 						
c. Is there a procedure to report disposition of arrests occurring after June 19, 1975 within the 90-day rule?								
3. Are there procedures for repository query by criminal justice agencies before CHRI dissemination? a. Are query requirements documented? b. Are written agreements with user agencies in existence?	 	 						
4. Are there procedures to maintain accuracy of records? a. Is notification on inaccurate information provided?	 	 						

Date of Certification: _____

OPERATIONAL PROCEDURE REQUIRED
BY PRIVACY AND SECURITY PLAN

[illegible]

PROCESS NO. (1, 2, 3, 4, 5, CENTRAL REPOSITORY)

AGENCY: _____

Date of Certification: _____

Person Conducting Certification

[illegible]

AGENCY: _____

Date of Certification: _____

Person Conducting Certification

[illegible]

AGENCY: _____

Date of Certification: _____

Person Conducting Certification _____

OPERATIONAL PROCEDURE REQUIRED BY PRIVACY AND SECURITY PLAN	A procedure is operational and:		Reason that procedure is not fully operational:				Estimated Date for procedure to be fully operational	
	Procedure meets Plan requirements	Procedure does not meet Plan requirements	No procedure is operational	Cost constraints	Time constraints	Technological	Lack of authority	
4. Is there a procedure for an individual to challenge the accuracy of his or her CHRI?	_____	_____	_____	_____	_____	_____	_____	_____
5. Is there a process for administrative review and record correction?	_____	_____	_____	_____	_____	_____	_____	_____
6. Are appeal procedures clearly identified?	_____	_____	_____	_____	_____	_____	_____	_____
7. Are correction procedures clearly identified?	_____	_____	_____	_____	_____	_____	_____	_____
8. Is the information subject to review clearly identified?	_____	_____	_____	_____	_____	_____	_____	_____
9. Will procedures be operational by March 16, 1976 which allow an individual to access and review his or her CHRI?	_____	_____	_____	_____	_____	_____	_____	_____

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

I certify that this certification is accurate.

Signed _____
(Head of Central Repository)

Signed _____
(Head of Agency)

END