

Utah Council on Criminal Justice Administration
Project on Criminal Justice
Standards and Goals

INFORMATION SYSTEMS

Privacy and Security

35253 DUP

Approved by
Utah Information Systems Task Force, and
Utah Council on Criminal Justice Administration
Room 304 State Office Building
Salt Lake City, UT 84114



GALVIN L. RAMPTON
GOVERNOR

STATE OF UTAH
OFFICE OF THE GOVERNOR
SALT LAKE CITY

NCJRS

October 11 1976

RECOMMENDATIONS

Dear Citizens:

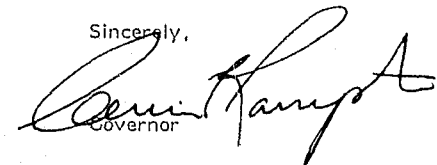
This pamphlet is one of a series of reports of the Utah Council on Criminal Justice Administration. The Council's five Task Forces: Police, Corrections, Judicial Systems, Community Crime Prevention, and Information Systems, were appointed on October 16, 1973 to formulate standards and goals for crime reduction and prevention at the state and local levels. Membership in the Task Forces was drawn from state and local government, industry, citizen groups, and the criminal justice profession.

The recommendations and standards contained in these reports are based largely on the work of the National Advisory Commission on Criminal Justice Standards and Goals established on October 20, 1971 by the Law Enforcement Assistance Administration. The Task Forces have sought to expand their work and build upon it to develop a unique methodology to reduce crime in Utah.

With the completion of the Council's work and the submission of its reports, it is hoped that the standards and recommendations will influence the shape of our state's criminal justice system for many years to come. Although these standards are not mandatory upon anyone, they are recommendations for reshaping the criminal justice system.

I would like to extend sincere gratitude to the Task Force members, staff, and advisors who contributed something unknown before--a comprehensive, inter-related, long-range set of operating standards and recommendations for all aspects of criminal justice in Utah.

Sincerely,


Governor

PRIVACY AND SECURITY

This report was published by the Utah Council on Criminal Justice Administration with the aid of Law Enforcement Assistance Funds.

INFORMATION SYSTEMS TASK FORCE

Marion Hazleton, Chairman	Art Christean Deputy Utah Court Administrator
Regnal Garff, Judge Second District Juvenile Court	Mrs. James B. Lee Citizen Representative
Robert Mullins, Reporter Deseret News	Mike Riordan, Director Planning and Research Salt Lake County Sheriff's Office
Ivard Rogers, Director Utah Bureau of Criminal Identification	Donald Spradling, Director Office of Emergency Services
David Young, Director Statewide Association of Prosecutors	

Task Force Staff

Mike Stewart

Arthur Hadachko

TABLE OF CONTENTS

Introduction	1
Standard 4.1 Security and Privacy Administration	2
Standard 4.2 Scope of Files	4
Standard 4.3 Access and Dissemination	4
Standard 4.4 Information Review	7
Standard 4.5 Data Sensitivity Classification	10
Standard 4.6 System Security	13
Standard 4.7 Personnel Clearances	16
Standard 4.8 Information for Research	19

PRIVACY AND SECURITY

The past several years have witnessed a substantial growth in both the number and size of criminal justice information systems. The Utah Criminal Justice Information System now collects, stores, and disseminates information concerning crimes, arrests, charges, prosecutions, convictions, sentences, correctional supervision, accused persons, stolen property, motor vehicle licenses, registrations, and similar data.

As the scope of such systems increase and as they become more automated, protection of privacy rights becomes increasingly important. Also, with the growing dependency of criminal justice personnel on automated files, this information becomes more susceptible to accidental or intentional invasion or injury. A lapse in the security of an information system could cause serious damage to criminal justice operations.

Security is seriously compromised when unauthorized persons can add to, change, or delete entries in the information system, when unauthorized persons can make extracts of information within the system for private motives or personal gains, or when the contents of the system or some portions of the contents can be made known to unauthorized personnel.

The term privacy refers to the protection of the interests of the peoples whose names appear for whatever reason in the contents of a criminal justice information system. The protection of individual privacy is a highly important concern in the development of any criminal justice information system. Constraints must be imposed on those systems to ensure that the highest practical level of protection is obtained.

Within these standards minimum acceptable levels of system security and privacy protection are established. These standards provide for legislation to support the security and privacy considerations of criminal justice information systems, limiting access and dissemination of information, right of information review and corresponding procedures, classification of data, security precautions, and research information from the system.

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 justice 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 criminal 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, currently 6 mos. by statute (1975 legislature), 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.

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 privacy in research programs. If any 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.

Raymond A. Jackson
Chairman

Robert B. Andersen
Director

UTAH COUNCIL ON CRIMINAL JUSTICE ADMINISTRATION (MEMBERSHIP)

D. Gilbert Athay
Attorney at Law

Gerald Bonser
Moab City Councilman

Melvin J. Burke, Commissioner
Uintah County Commission

Mrs. Barbara Burnett
Citizen Representative

George Buzianis, Commissioner
Tooele County Commission

Donald E. Chase, Commissioner
Box Elder County Commission

Kenneth Creer, Major
City of Springville

Judge Bryant H. Croft
Third District Court

Edgar M. Denny, Administrator
Department of Employment Security

Mayor Richard C. Diamond
Wasatch Front Regional Council

Roscoe Garrett, Commissioner
Jaub County Commission

Glen Greener, Commissioner
Salt Lake City Commission

Capt. Norman "Pete" Hayward
Salt Lake County Sheriff's Office

Marion Hazleton
Citizen Representative

Rex Huntsman
Sevier County Sheriff

Chief Joseph Hutchings
St. George Police Department

Raymond A. Jackson, Commissioner
Department of Public Safety

S. Mark Johnson, Judge
Bountiful City Court

Paul C. Keller, Judge
Juvenile Court, District Five

Reverend Jerald H. Merrill
Citizen Representative

J. Duffy Palmer
Davis County Attorney

Dr. Sterling R. Provost
Utah State System of Higher Educ.

Paul S. Rose, Executive Director
Department of Social Services

Walter D. Talbot, Superintendent
of Public Instruction

Robert B. Hansen
Deputy Attorney General

Ernest D. Wright, Director
Division of Corrections

James F. Yardley, Commissioner
Garfield County Commission

WHAT IS THE UTAH COUNCIL ON CRIMINAL JUSTICE ADMINISTRATION (UCCJA)?

In 1968 the Omnibus Crime Control and Safe Streets Act was passed resulting in the creation of the Law Enforcement Assistance Administration (LEAA) in the U.S. Department of Justice. The act required the establishment of a planning mechanism for block grants for the reduction of crime and delinquency.

This precipitated the establishment of the Utah Law Enforcement Planning Council (ULEPC). The council was created by Executive Order of Governor Calvin Rampton in 1968. On October 1, 1975, the council was expanded in size and redesignated the Utah Council on Criminal Justice Administration (UCCJA).

The principle behind the council is based on the premise that comprehensive planning, focused on state and local evaluation of law-enforcement and criminal-justice problems, can result in preventing and controlling crime, increasing public safety, and effectively using federal and local funds.

The 27-member council directs the planning and funding activities of the LEAA program in Utah. Members are appointed by the governor to represent all interests and geographical areas of the state. The four major duties of the council are:

1. To develop a comprehensive, long-range plan for strengthening and improving law enforcement and the administration of justice . . .
2. To coordinate programs and projects for state and local governments for improvement in law enforcement.
3. To apply for and accept grants from the Law Enforcement Assistance Administration . . . and other government or private agencies, and to approve expenditure . . . of such funds . . . consistent with . . . the statewide comprehensive plan.
4. To establish goals and standards for Utah's criminal-justice system, and to relate these standards to a timetable for implementation.

END

7 11/11/11