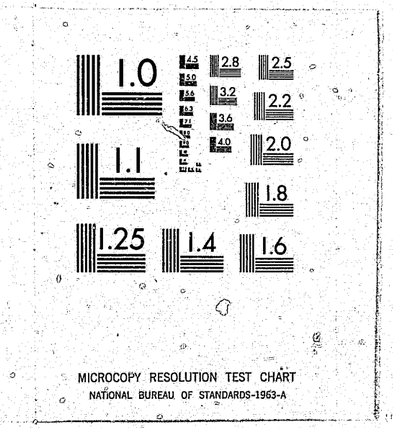
If you have issues viewing or accessing this file contact us at NCJRS.gov.

National Criminal Justice Reference Service

ncjrs

This microfiche was produced from documents received for inclusion in the NCJRS data base. Since NCJRS cannot exercise control over the physical condition of the documents submitted, the individual frame quality will vary. The resolution chart on this frame may be used to evaluate the document quality.



Microfilming procedures used to create this fiche comply with the standards set forth in 41CFR 101-11.504.

Points of view or opinions stated in this document are those of the author(s) and do not represent the official position or policies of the U. S. Department of Justice.

National Institute of Justice
United States Department of Justice
Washington, D.C. 20531

3/8/82

MF

LIBRARY COPY
Statistics Division, NCJISS

CRIMINAL JUSTICE SYSTEMS STANDARDS AND GOALS FOR SOUTH DAKOTA

80674

LIBRARY COPY
PROPERTY OF
LAW ENFORCEMENT ASSISTANCE ADMINISTRATION
DENVER REGION

SOUTH DAKOTA
STATISTICAL ANALYSIS CENTER

U.S. Department of Justice
National Institute of Justice

This document has been reproduced exactly as received from the person or organization originating it. Points of view or opinions stated in this document are those of the authors and do not necessarily represent the official position or policies of the National Institute of Justice.

Permission to reproduce this copyrighted material has been granted by

Public Domain, US Dept. of Justice
SD Statistical Analysis Ctr

to the National Criminal Justice Reference Service (NCJRS).

Further reproduction outside of the NCJRS system requires permission of the copyright owner.

CRIMINAL JUSTICE

SYSTEMS STANDARDS AND GOALS

FOR SOUTH DAKOTA

NCJRS
AUG 18 1981
ACQUISITIONS

RECEIVED
JUL 18 1977
REGION VIII
LEAA - DENVER

June, 1977

This document was printed to publish the report of the South Dakota Statistical Analysis Center on Criminal Justice Systems Standards and Goals for South Dakota at a per copy cost of $1.11

Prepared by

THE SOUTH DAKOTA STATISTICAL ANALYSIS CENTER

Criminal Justice Studies Program

University of South Dakota

Vermillion, S.D. 57069

James R. Villone.....Director

George Breed.....Coordinator

Diane Beecher.....Research Associate

Michel Hillman.....Research Associate

James Martin.....Research Associate

Sue Kracht.....Secretary

The publication of this report was made possible by grants from the Department of Justice, Law Enforcement Assistance Administration under the Omnibus Crime Control and Safe Streets Act of 1968, as amended (grant numbers: 76-SS-08-0002 and 76-ED-08-009). The points of view and opinions stated are those of the Statistical Analysis Center and the Systems Task Force and do not necessarily represent the official position or policies of the U.S. Department of Justice.

ACKNOWLEDGEMENTS

The Systems Task Force and the Statistical Analysis Center staff devoted considerable time and energy to developing the systems standards over the course of a year. Diane Beecher supervised the editing of these materials for publication, with the assistance of Carolyn Folta, John Lucas, Marya Manfred, Claire Sorenson and Sue Kracht.

Ralph Howenstine, Steven Long and Virginia Haluska were employed with the Statistical Analysis Center during this project and each of these individuals made a substantial contribution.

SYSTEMS TASK FORCE

Members

Chairperson: Captain Roger Hoffman-
Fiscal Officer
Highway Patrol
Pierre

Mr. Duane Anderson-
Assistant City Attorney,
Sioux Falls

Ms. Roxine Bown-
Brookings

Dr. Walter Busse-
Policy Analyst,
State Planning Bureau,
Pierre

Mr. Ralph Diggins-
Manager of Systems Development,
Social Services Department,
Pierre

Mr. Les Garry-
Director,
Central Data Processing,
Pierre

Mr. Tom Gerber-
Bureau of Administration,
Pierre

Captain David Green-
Sioux Falls Police Department,
Sioux Falls

The Honorable William Janklow-
Attorney General,
Pierre

Senator Homer Kandaras-
Rapid City

Ms. Doris Kessler-
Division of Criminal Investigation,
Pierre

Mr. James Melstad-
Director,
State Radio Communications,
Pierre

Mr. Robert Mines-
State's Attorney,
McIntosh

Dr. Max Myers-
Director,
Institute of Social Sciences for
Urban and Rural Research,
Brookings

Sheriff Willard Weiland-
Parker

The Honorable Marshall Young-
Circuit Court Judge,
Rapid City

Mr. David Zolnowsky-
Research & Development Officer,
Supreme Court,
Pierre

Liason

Ms. Joyce Emelio-
Criminal Justice Planning &
Development Officer,
Fourth District,
Aberdeen

Mr. James Rowenhorst-
Division of Law Enforcement
Assistance,
Pierre

CONTENTS

Contents (cont.)

INTRODUCTION

Systems standards, by definition, apply to the entire realm of criminal justice activities, from law enforcement through corrections. They are concerned with agencies' operations and interrelationships, especially with regard to the collection and use of information. Standards in this area are vital because the criminal justice "system" is loosely constructed with no single agency traditionally responsible for uniformity or inter-agency communications.

The Statistical Analysis Center was established to provide a coordinating influence among criminal justice agencies in South Dakota. Moreover, the initial thrust was toward data systems. For these reasons, and because of their expertise, the Advisory Committee to the Statistical Analysis Center served as the Systems Task Force.

The systems standards were formulated as part of a larger effort, the South Dakota Criminal Justice Standards and Goals Project. A companion volume, Criminal Justice Standards & Goals for South Dakota, focuses on the separate components of police, courts, corrections, community crime prevention, and reservations. All task forces met numerous times during 1975 and 1976, with research staff support, to adopt standards appropriate for South Dakota.

The Systems Task Force relied extensively upon a publication of the National Advisory Commission on Criminal Justice Standards and Goals, entitled Criminal Justice System. Where part or all of

a standard was deemed valid for South Dakota, the same or similar wording was used; where the commentary adequately expressed the committee's views, it was taken directly, in full or in part, from the national publication. Both reflect compromises dictacted by the state's special problems and needs. The implementation sections were specifically written for and tailored to South Dakota.

JURISDICTIONAL RESPONSIBILITY

Standard 1.1 Coordination of Information Systems Development

South Dakota should create an organizational structure for coordinating the development of information systems and for making maximum use of collected data in support of criminal justice management by taking the following steps:

1. Establish a criminal justice information planning and analysis unit that will coordinate the development of an integrated network of information systems in the State and will satisfy information needs of management decisionmaking for State and local criminal justice agencies as well as satisfying established Federal requirements for information.

2. While making provisions for continual review and refinement, prepare a master plan for the development of an integrated network of criminal justice information systems (including the production of data needed for statistical purposes) specifying organizational roles and timetables.

3. Provide technical assistance and training to all jurisdiction levels and agencies in data collection methods, system concept development, and related areas.

4. Arrange for system audit and inspection to insure the maintenance of maximum quality in each operating system.

Commentary

The emergence of computerized criminal justice information systems has occurred in many states without serious attention being given to the interrelationships between these systems. Neither have clear definitions of appropriate roles within these systems been formulated. This has resulted in substantial losses due to incompatible systems, and unneeded duplications of effort and money.

A separate unit, sufficiently removed from the day-to-day operating functions of other agencies, is required to combat this lack of organization. This unit must not only fill the gap in planning which presently exists but it must also make use of the criminal justice statistics which are the product of such a system.

State and local agencies cannot be expected to implement this system without some form of technical assistance and training. Such assistance must be available to insure that the quality of data is maintained and that information systems are properly implemented.

Implementation

A. Agencies Involved:

All criminal justice agencies maintaining, collecting, or in some manner exercising control over criminal justice information

State Criminal Justice Commission

Criminal Justice Statistical Analysis Center (SAC)

B. Administrative Actions:

While statutory authority would lend the proper amount of force to guaranteeing continued existence of the SAC, a well-supervised series of administrative decisions could accomplish similar ends.

C. Funding:

Until the State can assume responsibility for funding the SAC, the Law Enforcement Assistance Administration should be encouraged to provide such funding as may be necessary.

Standard 1.2 State Role in Criminal Justice Information and Statistics

Where feasible and appropriate, South Dakota 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 persons arrested for an NCIC-qualified offense, with on-line availability of at least a summary of criminal activity and current status of offenders;

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 (National Crime Information Center), 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 for all intrastate users and routing (formating) of messages to and from qualified agencies in other States;

7. The collection, processing, and reporting of Uniform Crime Reports (UCR) 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.

Commentary

Standard 1.2 defines the role of the State in South Dakota's criminal justice information system.

This standard establishes, where feasible and appropriate, the computerized common files needed by law enforcement personnel throughout the State. It recommends that computer-controlled communications links for agency-to-agency communications

be established, and it gives South Dakota the role of developing computerized criminal histories and an Offender-Based Transaction Statistics (OBTS) system.

Besides calling on South Dakota to initiate new programs at the State level, Standard 1.2 requests the State to take the initiative of making sure that UCR reports are collected and forwarded to the FBI.

Implementation

A. Agencies Involved:
   Office of Criminal Investigation
   Highway Patrol
   Central Data Processing
B. Legislation:
   Budget Appropriations must be promulgated by the agencies involved.
C. Administrative Actions:
   Coordination and implementation agreements must be fashioned.
D. Funding:
   The South Dakota Legislature and LEAA would be the primary funders.

Standard 1.3 Local Criminal Justice Information Systems

Every locality in South Dakota should be serviced by a local criminal justice information system which supports the needs of criminal justice agencies.

1. The Local Criminal Justice Information System (LCJIS) should contain information concerning every person arrested within that locality from the time of arrest until no further criminal justice transactions can be expected within the locality concerning that arrest.

2. The LCJIS should contain a record of every local agency transaction pertaining to a criminal offense concerning such persons, the reason for the transaction, and the result of each such transaction. A transaction is defined as a formal and public activity of a criminal justice agency, the results of which are a matter of a public record.

3. The LCJIS should contain the present criminal justice status for each individual under the cognizance of criminal justice agencies.

4. The LCJIS should provide prompt response to inquiries from criminal justice agencies that have provided information to the data base of LCJIS.

5. If the LCJIS covers a geographical area containing contiguous jurisdictions, it should provide investigative field support to police agencies within this total area.

6. LCJIS should provide a master name index of persons of interest to the criminal justice agencies in its jurisdiction. This index should include identifying information concerning persons within the locality under the cognizance of criminal justice agencies.

7. The LCJIS should provide to the proper State agencies all information concerning postarrest offender statistical data as required.

8. The LCJIS should provide to the proper State agencies all postarrest data necessary to maintain a current criminal history record on persons

arrested and processed within a locality.

9. If automated, LCJIS should provide telecommunications interface between the State CJIS and criminal justice agencies within its locality.

Commentary

Standard 1.3 provides the groundwork for the establishment of Local Criminal Justice Information Systems which transcend the boundaries of agencies within a certain locality, county, or counties.

The primary reason for the establishment of LCJIS facilities is to fulfill the need of South Dakota's law enforcement, prosecution, courts, and corrections personnel for prompt access to data concerning individuals and events within a locality. The goal of an LCJIS is to avoid duplication of data entry for data needed by more than one agency, to minimize the operating costs of making the data available, and to provide a single source for reporting to State and Federal systems.

The LCJIS is not intended to deny or restrict the larger cities or counties from developing their own component systems, but rather to promote the logical development of systems that best serve the users.

Implementation

A. Agencies Involved:
   Incorporated counties in South Dakota
   Major South Dakota cities
B. Administrative Actions:
   Cooperation between all criminal justice agencies at the local level must occur.
C. Funding:
   LEAA, the South Dakota Legislature, and individual county and city law enforcement budgets will be contributing to the establishment of local information systems.

Standard 1.4 Criminal Justice Component Information Systems

Every component agency of the criminal justice system (police, courts, corrections) should be served by an information system which supports its intraagency needs.

1. The Component Information System (CIS) should provide the rationale for the internal allocation of personnel and other resources of the agency.

2. The CIS should provide a rational basis for scheduling of events, cases, and transactions within the agency.

3. The CIS should provide the agency administrator with clear indications of changes in workload and workload composition, and provide the means of distinguishing between short-term variations (e.g., seasonal variations) and long-term trends.

4. The CIS should provide data required for the proper functioning of other systems as appropriate, and should retain only that data required for its own specific purposes.

5. The CIS should provide the interface between LCJIS and individual users within its own agency. This interface provision should include telecommunications facilities as necessary.

6. The CIS should create and provide access to files needed by its users that are not provided by the State or local criminal justice information systems to which it is interfaced.

7. The CIS should support the conduct of research and program evaluation to serve agency managers.

Commentary

The Component Information Systems are designed to serve the needs of agency administrators. The CIS consists of operational files in police, courts, and corrections systems which more than likely are unique to those systems. The CIS should be designed to meet the needs of the agencies' managers and operational users, but with the constraint of not duplicating those information services available through an LCJIS.

It must be kept in mind that users within an agency may use not only the LCJIS but other information systems also.

The assignment of jurisdictional responsibility covers both manual and automated systems, and does not imply that automation is necessary. This standard primarily suggests that component systems should focus on satisfying internal needs which are not proper subjects for inclusion in a local or State criminal justice information system.

Implementation

A. Agencies Involved:
   All law enforcement agencies, State and local
   State's Attorney Offices
   Judiciary Department
   All correctional institutions, State and local
B. Funding:
   The State Legislature should react favorably toward those agencies that wish to either implement or upgrade automated systems. Of course, it should be indicated that in many cases manual systems will suffice, so appropriations may be lessened and still accomplish the desired goals.

POLICE INFORMATION SYSTEMS

Standard 2.1 Police Information Systems

Every police agency should have a well-defined information system. Proper functions of such a system include:

1. Dispatch information, including the generation of data describing the dispatch operation and data useful in the dispatching process;

2. Event information, including the generation and analysis of data on incidents and crimes;

3. Case information, including data needed during follow-up until police disposition of the case is completed;

4. Reporting and access to other systems which provide required data for operational or statistical purposes; and

5. Patrol or investigative support data not provided by external systems, such as misdemeanor want/warrant data, traffic and citation reporting, and local property data.

Commentary

These five basic functions, when combined with the capabilities of external systems, provide the police department with the information essential to operations and management. Systems should be designed to support resource allocation and crime analysis, as well as other administrative needs of a police department. Careful consideration of the design and the data elements that are to be stored is essential if information use is to be effective.

Information is the basic tool in the operation of a police department from both an administrative and a tactical planning viewpoint. It must be one of every department's higher priorities.

The dispatch information function increases the efficiency of unit assignment and also provides a record of the police response to a call for service, including elapsed time.

The event information should support all agency needs for crime data and generate Uniform Crime Reports (UCR) and other reports as a by-product.

Case information, including the necessary indexes to offenders, victims, and events; the status of follow-up investigation; and the scheduling of prosecutorial and court actions are needed to support management as well as individual investigatory decisions.

The other systems referred to in part 4 above might provide data on the criminal justice system (e.g., Offender-based Transaction Statistics, or OBTS), data on behavior (e.g., alcoholism and drug abuse), data on the environment (e.g., land typology), and methodological tools (e.g., geocoding).

Some departments do not report "noncrime" dispositions in any detail. When a patrol is called into service, it simply states that no report is required. Therefore, the basis for audit is not as accurate as more detailed information on the reasons for not reporting.

Implementation

A. Agencies Involved:
All law enforcement agencies, State and local

B. Legislation
When considered together, the state radio system and teletype network form a solid base with regard to this standard. An expansion of such services would be best accomplished by enabling legislation, particularily where funding will be necessary. Legislation presently exists which empowers the Attorney General to create and maintain the state radio and teletype systems. It may, therefore, be a relatively simple matter to administratively expand the quantity and quality of transmitted information.

In order to provide data on court actions (dispositions, etc.) an arrangement (statutory if necessary) with the court information system will certainly be necessary. The question of information exchange will have to be dealt with by any two agencies that wish to use each other's data.

C. Funding
The Attorney General is, by statute, authorized to expend funds on such information systems as contemplated by the standard.

Standard 2.2 Crime Analysis Capability

Every police department should improve its crime analysis capability by utilizing information provided by its information system within the department. Crime analysis may include the utilization of the following:

1. Methods of operation of individual criminals;

2. Pattern recognition;

3. Field interrogation and arrest data;

4. Crime report data;

5. Incident report information;

6. Dispatch information; and

7. Traffic reports, both accidents and citations.

These elements must be carefully screened for information that should be routinely recorded for crime analysis.

Commentary

The purpose of crime analysis is to support investigative operations, field operations, and administration on a day-to-day basis, and when possible, to prepare management information statistics. It involves crime data collection, crime data correlation, analysis, dissemination, feedback and evaluation. Pattern recognition has two dimensions, both essential to reduce crime. The first attempts to recognize a specific pattern of criminal activity, such as in burglary. The second is much broader and recognizes a general crime picture developing in areas of a jurisdiction.

Characteristically, crime analysis has been crime-event-oriented and has ignored data routinely stored in police files, data which is unavailable to the crime analysis team because of the storage methods used. Routine information filed in police departments should be carefully analyzed for all possible uses, and the crime analysis package should be designed to view the activities of the department through one comprehensive viewpoint.

Where the size of a department and its resources argue against expansion of crime analysis capability, agencies external to the department could process and analyze data for the department's internal use. Guidelines should be developed to indicate the types and extent of crime analysis appropriate for agencies of various sizes and with various crime rates. Even a one-person department can benefit by adopting an attitude of systematic inquiry with regard to the information it holds.

Implementation

A. Agencies Involved:
All law enforcement agencies, State and local

B. Administrative Actions:
Each agency must begin first to collect and maintain complete information before it can hope to derive any benefit from analysis. Such collection efforts may have to begin at the command level of each law enforcement agency. Reluctance to inititate data collection independently should be countered by decisions from upper echelons or by statutory authority. (It should be noted that fingerprint cards are required by South Dakota statute, yet not all agencies comply with this provision.)

C. Funding
A combination, if necessary, of State, county, and municipal funds may be utilized to provide the necessary facilities and personnel for management of data that has been collected. This arrangement assumes that some agencies will have manual systems. Funding may also be used to insure compliance with directives; unsatisfactory data collection may be met with a slightly reduced budget.

Standard 2.3 Personnel Resource Allocation and Control

Police agencies should develop personnel resource allocation and control systems that will support major efforts to:

1. Identify through empirical means the need for personnel within agencies;

2. Provide planning for maximum utilization of available resources;

3. Provide information for the allocation and instruction of patrol officers and specialist officers; and

4. Provide for the evaluation of adopted plans.

Commentary

Personnel resources cannot be effectively allocated without sufficient input data--data gathered routinely over a significant period of time. The basic data in a patrol workload reporting system are the time and date a call is received, the address of the incident, the incident type, the cars dispatched and times of dispatch, and the time(s)service is terminated. Use of this data

and of crime analysis information along with a close examination of the goals appropriate for the agency and the community under consideration will facilitate personnel resource allocation and control.

Objectives of patrol distribution may include diminishing opportunities for criminal acts, shortening response-distance arrival-time, equalizing suppressive patrol time and training and exposure hazard among patrol officers, increasing the likelihood of assistance from one officer to another, and concentrating officer strength in the areas where more police control should occur. Personnel resource allocation is predicated on determining the type of police service required and its distribution in space and time. Personnel resource control builds upon successful personnel allocation. Allocation deals with gross areas (i.e, beats) and large blocks of time (i.e., shift duration), satisfies routine needs, and is concerned largely with police response in relation to events already completed. In contrast, control deals with the detailed actions of individual officers, satisfies unexpected or varied needs, and is concerned primarily with crime prevention and apprehension of criminals during criminal acts. A personnel control system would provide a list of individual crime-prone locations to be investigated and specific times for each investigation.

Personnel resource allocation and control are used to optimize performance and aid in the reduction of crime. When information from command and control is available, a large portion of preventive control can and must be directed by a command center. For those agencies which are too small to adequately study their own personnel needs and engage in short-and long-term planning, there must be leadership exerted by law enforcement agencies and organizations so that systems applicable to the small agencies are designed and evaluated. No matter how simple or basic the proposed system, the crucial factors are that it would be a conscious attempt to examine personnel problems and that it would be based on the needs of the area served.

There is little sound research in this complex area, and the unique aspects of any department would require evaluation of the application of even widely tested methods of allocation and control. Evaluation is a difficult concept to promote. It must be considered a tool of a professional law enforcement agency, not a judgement of performance. The judgment should be directed at the methodology by which resources have been allocated, not at the effectiveness of individual officers. If evaluation is viewed negatively, then the effect of planning, allocating, and controlling of patrol activity will be lost. Only by evaluating planned approaches and viewing their results can the tool of resource allocation bring about the reduction of crime.

Implementation

A. Agencies Involved:
All law enforcement agencies, State and local, plus associated governmental bodies

B. Funding:
Funding should be sought from the Law Enforcement Assistance Administration (LEAA) to conduct such a study where the size of the police department requires outside evaluation. The State or county should be responsive to police agencies that wish to improve delivery of services.

Standard 2.4 Police Information System Response Time

Information should be provided to users in sufficient time to affect the outcome of their decisions. The maximum allowable delay for information delivery,

measured from initiation of the request to the delivery of a response, varies according to user type.

1. For users engaged in unpredictable field activity of high potential danger (e.g., vehicle stop), the maximum delay should be 120 seconds.

2. For users engaged in field activity without direct exposure to high potential danger (e.g., checking parked vehicles), the maximum delay should be 5 minutes.

3. For users engaged in investigatory activity without personal contact (e.g., developing suspect lists), the maximum delay should be 8 hours.

4. For users engaged in postapprehension identification and criminal history determinations, the maximum delay should be 4 hours.

Commentary

Most information systems are designed to establish response priorities by type of data requested rather than by type of user. Thus an officer making a "wanted check" during a vehicle stop, and another officer making identical checks on parked or abandoned cars, receive the same response priority despite the different degree of danger to which they are exposed. There is also a tendency to establish response time criteria of "as soon as possible" rather than of specific acceptable delays. Establishment of inquiry codes and segmented inquiry queues would alleviate these problems.

State Radio and the Division of Criminal Investigation (DCI) can now respond within these maximum allowable delays, under optimum conditions. However, dispatchers use their discretion and experience to determine priority levels and response times, rather than formalized rules. This standard applies not only to state-level responsiveness to inquiries from local systems, but also to the ability of the local systems to provide their own information to their own officers within acceptable time limits.

Implementation

A. Agencies Involved:
All law enforcement agencies, State and local

B. Funding:
Much of the standard depends in part upon more sophisticated information delivery and categorization systems. On the local level, in particular, before agencies can worry about minimum response times, a commitment must exist to upgrade collection and processing of data; the key, of course, is for an agency to receive the funds to accomplish these objectives on a continuing basis.

Standard 2.5 UCR Participation

Every police agency should, as a minimum, participate fully in the Uniform Crime Reporting program.

Commentary

Participation means collecting the required data, processing it (classifying crimes, and so on), and reporting to a higher level for aggregation. The FBI has been encouraging each state to collect the data from all police agencies in the state and then make a single submission to the FBI; the DCI is working on such an arrangement for South Dakota. This standard urges cooperation with the change to state-based reporting, and implicitly recognizes that exhausive reporting is necessary for the success of the program. South Dakota does not have a law mandating participation and the data which has been gathered has not been sent to a central place in the State so that crime trends and problems could be examined. More widespread reporting and availability of data on the State level would allow the information to be put to use for the state rather than merely passed on to the Federal level.

Implementation

A. Agencies Involved:
All law enforcement agencies, State and local, with special emphasis on the Division of Criminal Investigation
Criminal Justice Statistical Analysis Center

B. Legislation
SDCL 23-6-12 (Cooperation of Bureau with Federal Government...) indicates that the State shall participate in developing a system of criminal identification; however, there is no statutory provision requiring compliance with the FBI's request for UCR data. The validity of UCR data is not presently under consideration by the standard; the important point is to accumulate usable data.

C. Administrative Actions:
Barring creation by statute, coordination of efforts to supply UCR data could be accomplished by an opinion from the Attorney General and through the DCI and by assistance from the Statistical Analysis Center and the FBI for technical aid and/or training. Because many police departments are small and are spread out over great distances in South Dakota, coordination and planning will be necessary to make the system function properly.

D. Funding:
Again, while not recommended except as a last resort, monetary pressure can be used in order to force compliance from more recalcitrant agencies. Consideration should be given to the use of existing expertise. The Statistical Analysis Center, the Attorney General's staff, and larger police departments can supply the needed expertise.

Standard 2.6 Expanded Crime Data

For use at the local level, or for State and regional planning and evaluation, data collected concerning an incident regarded as a crime should include as a minimum:

1. Incident definition, including criminal statute violated and UCR offense classification;

2. Time, including time of day, day of week, month, and year;

3. Location;

4. Incident characteristics, including type of weapon used, method of entry (if applicable), and degree of intimidation or force used;

5. Incident consequences, including type and value of property stolen, destroyed, or recovered, and personal injury suffered;

6. Offender characteristics (each offender), including relationship to victim, age, race, sex, residency, prior criminal record, criminal justice status (on parole, etc.), employment and educational status, apparent intent, and alcohol/narcotics usage history;

7. Type of arrest (on view, etc.); and

8. Witnesses and evidence.

The data should be obtained at least for murder, forcible rape, robbery, aggravated assault, and burglary (both residential and commercial).

Commentary

The routine procedures required for the conduct of criminal justice business can provide the necessary data for the most basic information system. More detail is required than that which enters the UCR system, and the elements mentioned in this standard are widely regarded as data which must be collected. Universal factors for crime analysis have been classified as crime type, geographical, chronological, victim target descriptive, and property loss descriptive. As long as it is understood that the standard sets up a minimum level of data collection and there are considerable precedents and reasons for expansion, its brevity makes it easier for even the smallest department to comply.

Offender characteristics must be described for use in correctional information systems. To the extent that these and other data are available from other systems, the collection effort should not be duplicated and the information should be shared.

Expanded crime data are needed for problem identification, effective allocation of resources, and evaluation of new programs. Data needs change as different and new ways of focusing on the more serious crime problems are developed. Crime specific planning, for example, demands more detail on the event than have past planning models.

To direct an adequate program against specific crime, the distribution and characteristics of the criminal events should be determined. To allocate resources effectively the distribution of offenses must be examined in terms of both time and space. In such a study, it is important to know the times of day when the target offenses occur, as well as the days of the week, and to some extent, the season of the year.

It is equally important to know where crimes occur. Response tactics and strategies will vary, depending upon whether the crimes occur on the street or elsewhere, and by the type of place in which off-street crime occurs, e.g., liquor stores, filling stations, apartment buildings, or public transit. The area or neighborhood in which street crimes occur is also important.

Beyond the specifics of time and location, data on the characteristics of the event can often provide tactical direction. Information about the number of offenders, their apparent age, weapons, and so on, can be useful. For planning, too much reliance on the usual classification of offenses can be counter-productive. Thus, for example, one might cite the intended offense as well as the most serious offense that occurred during a criminal incident.

The primary source of information about offenders is the arrest record.

While there is no assurance that the characteristics of persons arrested are representative of all those committing similar offenses, we have little choice but to use arrest statistics as a substitute for true offender statistics. In describing "all offenders," using data derived from "offenders apprehended," we may make mistakes in analysis. The only alternative, unfortunately, is no analysis. Arrest data used in conjunction with incident reports can produce estimates of offender characteristics for crimes within specific areas. Arrest rates must be used with extreme care; a primary measure should be "effective arrests"--those which result in prosecutable cases.

Implementation

A. Agencies Involved:

All agencies involved in the collection or maintenance of criminal justice data, but with special emphasis on law enforcement agencies, State and local

B. Administrative Actions:

An effort aimed at standardarizing the method of collection, type (variety) of the data, and storage requirements should be initiated across the State at all levels of law enforcement. Statutory authority would necessarily have to be vague as it presently is, in order to allow agencies the requisite discretion to successfully accomplish their jobs. The force of such a move toward standarization should originate from a source common to all agencies such as the Governor's Office, or from the Attorney General's Office.

C. Funding:

Again, funding may provide an unpleasant but necessary lever to promote compliance.

Standard 2.7 Quality Control of Crime Data

Every police agency should make provision for an audit of incident and arrest reporting. The audit should verify that:

1. Crime reports are being generated when appropriate;

2. Incidents are being properly classified; and

3. Reports are being properly prepared and submitted.

Commentary

The success of an information system is reflected in the usefulness of the crime analysis component, which in turn is based upon the kind, accuracy and completeness of data input. To assess the quality of the data and determine where improvement or correction is needed, audits of incident and arrest statistics should be routinely carried out. This is essential in order to maintain the integrity and credibility of crime statistics.

The audit program is intended to identify and correct sources of error, not to verify the honesty or integrity of the reporting unit. There are sources of error in any statistical program--interpretation of instructions, method of asking questions and recording answers, and steps in processing the original reports to the final format of the statistical tables. A quality control program will sometimes help find the sources or the extent of errors.

Whenever possible, report review processes and audit trails should complement and support the audit program. Report review consists of editing reports,

reviewing their contents, determining the effectiveness of the report flow process, classifying events, initiating corrective actions, assuring proper distribution and routing of reports, and evaluating the effectiveness of the report system. This permits checking on a regular basis and insures that the audit's verification procedure will periodically reveal a small number of random or systematic errors rather than a host of problems which require drastic measures. In order to verify the accuracy of reports in relationship to the facts of events and to provide basic documentation needed by management, all police responses should be recorded (whether the event is classified as crime or noncrime, or the assignment is self-initiated, etc.) and dispatch and other reports should be numbered to facilitate their linkage.

Implementation

A. Agencies Involved:
All law enforcement agencies, State and local
Criminal Justice Statistical Analysis Center

B. Administrative Actions:

A commitment from those in charge of each agency is necessary to insure that the proper records are kept and audits are anticipated. In order that comparable standards adhere throughout the law enforcement system, external audits should supplement regular internal audits. Thus, for external audits or where agencies have difficulty conducting internal audits due to lack of trained personnel, the services of the SAC should be called upon.

C. Funding:

Administrators and employees should receive training in audit procedures, perhaps through the DCI and funded by the Attorney General's Office. Some agencies may need one-time budget supplements to reorganize their records and procedures, but most agencies large enough to conduct internal audits have the requisite staff and budget. Funds for externally conducted audits could initially be requested from LEAA, but eventually the State would have to insure quality control.

Standard 2.8 Geocoding

Where practical, police should establish a geographical coding system that allows addresses to be located on a coordinate system as a basis for collecting crime incidence statistics by beat, district, census tract, and by other "zoning" systems such as schools, planning zones, and zip codes.

Commentary

This standard calls for the development in medium and large jurisdictions (e.g., more than 100,000 population) of a computerized geographical coding system. The best and most readily available system in many cities is the Geographic Base File (GBF) developed by the Bureau of Census. In this system, each record in the file describes a straight line segment with the following information:

1. Coordinates at each end;
2. Tract and block number on each side;
3. Other geographical codes (such as precinct) on each side;
4. Name of the line (such as street, railroad, water feature, or political boundary); and

5. Address ranges on each side (when applicable).

A GBF can provide data in fine geographic detail for planning and evaluation. More important, it becomes a useful tool in determing day-to-day and hour-by-hour allocation of patrol personnel. It can be used in the dispatch process or to retrieve geographic information for investigative purposes. It can be used to match or compare data from police operations against data from other departments.

Geographic Base Files, with the appropriate computer and ancillary equipment, can draw maps with crime rate information or spot maps recording specific incidents. Through crime maps or tables, the location-based file can highlight areas with concentrations of various incidents by seasons, as required by police administrators.

Under the most advanced application of such maps, the computer together with an administrator having other specialized information can suggest changes in beat assignments on the basis of expected workloads. Geocoding forms the basis for computer-aided dispatching systems, and is useful as an investigative tool for various geographical matching problems.

A detailed level of geocoding is essential in scientific experimentation or program evaluation, where definition and measurement in experimental versus control areas is anticipated.

Geographic Base Files are used by other local agencies as well. Some of these may not be compatible with the needs of the police agency. However, the costs to the police agency of having an existing or a forthcoming system upgraded to meet its needs would be substantially less than the costs of completely independent projects. If the police are using the same GBF as other city agencies, it would be possible to compare police data with data from school systems, health and welfare departments, and engineering and building code departments. Also, results from the census, such as demographic and housing characteristics, will be available for areas defined by police administrators.

The census approach is a by-product of the technique of taking the 1970 census by mail. The Dual Independent Map Encoding (DIME) file is developed by entering each street or road segment, other line segments, such as railroads, streams and political boundaries, the "nodes" where these line segments intersect, and the block number for the areas bounded by the segments. Further, the highest and lowest numbered street addresses in each street segment are entered, as well as tract number and local codes as selected by the local agencies. The street address, which is usually on any incident report, is the only geographic code required for the DIME system.

Implementation

A. Agencies Involved:

Law enforcement agencies in towns or counties with over 100,000 people (presently Minnehaha County/Sioux Falls) or in the State (e.g., Highway Patrol)

B. Funding:

Geocoding systems exist in Sioux Falls and at the Highway Patrol. Given their value in planning and analysis both for law enforcement and for other governmental agencies, these systems should be taken advantage of more fully and shared. For increased use, the holding agencies will have to enlarge their budgets. Agencies sharing the systems will have to allocate money for such a purpose. No other systems need be established in the near future.

COURT INFORMATION SYSTEMS

Standard 3.1 Decisionmaking in Individual Cases

A court information system should provide information unique to the defendant and to the case. Useful information includes:

1. Defendant background data and other characteristics needed in decision-making such as defendant's family status, employment, residence, education, past history, indigency information relative to appointment of counsel, and such data as might be determined by a bail agency interview.

2. Current case history stating the proceedings already completed, the length of time between proceedings, continuances (by reason and source), respresentation, and other participants.

Information should be made available only to those who need and have a right to know including court workers, officers of the court, and the defendant, at the appropriate time.

All copies of the information referred to in section 1 which are not made part of the permanent court record or required by law should be periodically purged to insure that information is current and accurate.

Commentary

In each individual case current information on the defendant's employment, residence, family status, etc., is relevant to decisionmaking for such matters as bail setting, bail reduction, release on own recognizance, approval of negotiated pleas, and sentencing. The past criminal history of the defendant is also essential and should be included.

In order to protect the privacy of the defendant, all data collected in any form by the court information system should be made available only to those who need to know and have a right to know and only at a time appropriate to each case. To insure the accuracy of information about the defendant's background and to guard against the compiling of individual dossier files, all copies of such information which are not made part of the court record or are not required by law should be purged periodically and new information gathered if needed for another case.

Information about the individual case before the court increases the opportunity for effective prosecution and fairness to all parties. With verified information on the history of each, judges could control the granting of continuances and the scheduling of cases which might create attorney conflicts.

Implementation

A. Agencies Involved:
Judiciary Department

B. Administrative Actions:
Court order will suffice in terms of prompting personnel to comply with the section dealing with purging. There is no real need to compel courts to collect data because an adequate job is presently being done.

Until the courts have had sufficient time to implement, test and evaluate the information system presently under construction, external decisions or action should be held to a minimum.

C. Funding:
Closely allied with funding is provision of technical expertise. The

Statistical Analysis Center (SAC) should undertake to offer whatever technical advice or professional assistance it can.

Standard 3.2 Calendar Management in the Courts

Criminal courts should be provided with sufficient information on case flow to permit efficient calendar management. Basic data to support this activity include the following:

1. Periodic disposition rates by proceeding; these statistics can be used to formulate and adjust calendar caseload limits;

2. An age index of all cases in pretrial or awaiting trail (by type of trial requested) to determine if special attention is required or the speedy trial rule endangered;

3. An index relating scheduled cases to whether the defendant is confined, released, rearrested, at large, or undergoing adjudication on a separate offense;

4. A recapitulation of offenders booked in jail but not released, to determine if special attention is required.

Commentary

Strong calendar management by the courts is a major factor in eliminating delay and congestion. Much of the criticism directed at delay in courts relates to the calendar management function. These criticisms range from assembly line justice to delay in adjudication; they include the massing of defendants in crowded courtrooms and long waiting times for attorneys, defendants, and witnesses. Overset calendars-- by scheduling more than one trial to be held at the same time in the same courtroom--and the granting of an excessive number of continuances are two other problems in calendaring cases. While each of these problems in calendaring are relatively rare in South Dakota, they do occur and the information system needs to address them.

Calendars of optimum size, scheduled with a minimum of conflicts, are a reasonable management goal. The information required for this function can also provide the data base for automated completion of such regular judicial paper work as dockets and indexes.

Implementation

A. Agencies Involved:
Judiciary Department

B. Administrative Actions:
Legislation need not be obtained for implementation. A decision by the court administrator or chief justice will doubtless suffice. Statutory authority presently exists for the presiding judge of the circuit court to arrange and supervise calendaring (SDCL 16-2-2, SL, 1975). It is assumed that this statute also provides authority to request an analysis of data to improve such calendaring.

Standard 3.3 Court Management Data

For effective court administration, criminal courts must have the capability to determine monthly case flow and judicial personnel workload patterns. This capability requires the following statistical data for both in misdemeanors and felonies:

1. Filing and disposition--number of cases filed and the number of defendants disposed of by offense categories;

2. Monthly backlog--cases in pretrial or preliminary hearing stage; cases scheduled for trial (by type of trial) or preliminary hearing; and cases schedules for sentencing with delay since previous step in adjudication;

3. Status of cases on pretrial, settlement, or trial calendars--number and percent of cases sent to judges; continued (listed by reason and source), settled, placed off-calendar; nolle prosequi, bench warrants; terminated by trial (according to type of trial);

4. Time periods between major steps in adjudication, including length of trial proceedings by type of trial;

5. Judges' workload--number of cases disposed of by type of disposition and number of cases heard per judge by type of proceeding or calendar.

Commentary

Applying modern management and administration techniques to the courts is a fundamental step in the promotion of efficiency and equitable handling of the criminal caseload. Information is a tool of effective court management. A great many courts today are plagued with congestion and drawn out handling of cases. In addition to inefficient calendar management, causal factors are limited physical resources, a high rate of jury trials, and attorney attitudes. The results are delay of due process and a growing loss of public respect.

The application of modern management and administration techniques to alleviate these problems depends on the availability of information about what courts actually do. Most court systems lack information about their personnel, products (i.e., case dispositions and judicial workloads), facilities, and the various participants in the court's processes.

Appropriate management information systems can provide these kinds of data. Their users are able to make sound decisions based on valid current information; they can foster the best use of money, manpower, and material in daily operations. They can determine what policies to adopt and can measure the results of policy adoption.

The measurement of judicial workloads for weighting purposes, while possibly useful for management, has been in practice so cumbersome and expensive that wieghting caseloads is not recommended for South Dakota.

Implementation

A. Agencies Involved:
   Judiciary Department
B. Administrative Actions
   Until the full potential of the court information system has been explored,

it is difficult to speculate as to what data the courts are actually without. Among other reasons, the lack of such information prompted the creation of a court information system. It should be pointed out, however, that wherever practical the SAC should lend its assistance.

Agreements may also be worked out whereby an interface between the law enforcement information system and the court information system may be "built-in" to promote information exchange. Appropriate safeguards of privacy should be recognized as an integral part of any such arrangement.

Standard 3.4 Case Management for Prosecutors

For the purpose of case management, prosecutors shall be provided with the data and statistics to support charge determination and case handling. This capability shall include, as appropriate, the following:

1. Daily calendar worklo[illegible]s and dispositions;

2. Age of cases in pretrial or awaiting trial (by type of trial) to determine in part whether the right to a speedy trial is enforced;

3. Case schedule index listing police witnesses, expert witnesses, defense counsel, assigned prosecutor, and type of hearing.

Commentary

For case management, prosecutors need a system of information on case flow and statistical characteristics for their entire caseload. Several successful systems, including PROMIS, JURIS, PACE, and LEXIS, were reviewed. Unfortunately all of these computer-based systems require far higher caseloads than we have in South Dakota, even in Sioux Falls, to be economically feasible at this time. Therefore manual systems, involving cooperative efforts by State's Attorneys and the court's manual and automated information systems, should be utlized until automated systems for prosecutors become feasible.

The courts should provide the State's Attorneys with all information necessary for case management; however, the offices of the State's Attorneys should be responsible for the maintenance of the information. Calendar workloads and dispositions should be provided by the court sufficiently often (perhaps weekly in the smaller jurisdictions) to enable the State's Attorneys' offices to maintain daily case lists.

State's Attorneys should also bear some responsibility for the efficient movement of cases. Although case calendaring is a function of the courts in South Dakota, the State's Attorneys can contribute significantly to case flow through expeditious management of those resources and policies which they control. Charging practices, for example, have a significant effect on court workloads. With regular information on patterns of case flow, State's Attorneys can identify bottlenecks, allocate resources, and modify dubious policies.

State's Attorneys should also be notified by the court of the age of pretrial cases and cases awaiting trial, classified as felony or misdemeanor cases, in order to guarantee to the defendant his right to a speedy trial.

Finally State's Attorneys, with the help of the court, should prepare and maintain a current case schedule list detailing witnesses, defense counsels, prosecutor assigned, and type of hearing.

Implementation

A. Agencies Involved:
State's Attorney Offices
Judiciary Department
Office of the Attorney General
State Bar Association

B. Administrative Actions:

Legislation would not be necessary if the Office of the Attorney General would issue an administrative recommendation to all State's Attorneys and the Chief Justice were to perform the same action within his sphere of influence. Special interest groups, such as the State Bar Association, could be instrumental in pressing for such change.

C. Funding:

For computer-assisted systems that may ultimately be developed, Federal, State, and county funding (in collaboration) will be necessary. Interface with the court information system will also be necessary, and costs can perhaps be divided among various user agencies as required.

Standard 3.5 Research and Evaluation in the Courts

To create the capability for continued research and evaluation, courts should participate in or adopt for their own use a minimum set of data on the transactions between defendants and various court agencies including the outcome of such transactions, as determined by the offices of the Chief Justice and Court Administrator in cooperation with the Criminal Justice Statistical Analysis Center.

Commentary

South Dakota's Court is now planning and implementing a Judicial Information System to provide management and research information to the Court. This system has plans to provide information necessary for a statewide Offender-Based Transaction Statistics (OBTS) System and will be made compatible with any such system when adopted by South Dakota, as determined by the Office of Court Administration in cooperation with the SAC. Other statistical and informational research and evaluation work should be planned and implemented as needed by the Office of Court Administration.

Implementation

A. Agencies Involved:
Judiciary Department
Criminal Justice Statistical Analysis Center
Office of the Attorney General

B. Administrative Actions:

The Court in South Dakota is presently developing its own information system and will untimately participate in the statewide OBTS system. The SAC stands ready to assist in any fashion possible. Interface with the law enforcement information system would be of optimal value. The various agencies involved should be apprised of the potential value of information exchange. The same agencies should also be notified of the potential abuse that may result from information exchange conducted without adequate guidelines to insure privacy and security.

C. Funding:

Where technical or research expertise for planning and implementation is required, the Statistical Analysis Center can provide such expertise at a minimum cost to the State agencies involved.

Standard 3.6 Case Counting

Transactional and event data elements shall be recorded for counting purposes as follows: Data elements that describe events occurring in the criminal justice system shall record the number of events and the number of defendant transactions involved. Those data elements shall report the number of individual transactions as an additional explanatory item.

Under this standard, if two men are charged for the same criminal activities, this is reported as one charge with two defendants. If two charges are consolidated at one trial, it is to be reported as one trial on two charges. If a jury trial is held for three men for the same crime, the event should be reported as one jury trial for three defendants.

Commentary

In order to provide and report OBTS in a manner uniform throughout the United States, the South Dakota Judicial Information System should be capable of distinguishing individual defendants and charges. At the same time the information system should be capable of consolidating charges and defendants for reporting trial and caseload statistics in regard to consolidated trials. These capabilities are planned in the current Judicial Information System.

Implementation

A. Agencies Involved:
Judiciary Department

CORRECTIONS INFORMATION SYSTEMS

Standard 4.1 Development of a Corrections Information System

A corrections information system must satisfy the following requirements:

1. The information/statistics functions of offender accounting, administrative decisionmaking, ongoing research, and rapid response to questions should be supported.

2. The information now used or needed by corrections personnel at each decision point in the corrections system should be ascertained before the information system is designed.

3. The requirements of other criminal justice information systems for corrections data should be considered in the data base design. Interface between the corrections system and other criminal justice information systems should be developed.

Commentary

The corrections information system should be designed to support the management functions outlined in this standard. This system should be designed so that its data base is broad enough to incorporate future changes and so that the overall system is compatible with other criminal justice information systems.

State and local agencies cannot be expected to develop this system without some guidelines. It is therefore recommended that national guidelines for correctional information systems be used to assist these agencies in the establishment of an adequate data base.

Implementation

A. Agencies Involved:
Judiciary Department
All correctional institutions, State and local
Board of Charities and Corrections
Board of Pardons and Paroles
Office of the Attorney General
Criminal Justice Statistical Analysis Center
Agencies not officially designated as Correctional but that collect, maintain or in some other fashion utilize corrections information

B. Legislation

Doubtless the most efficient and effective method for the creation of an outstanding corrections information system is to legislate a unified corrections system, state-wide. It is not so much **that** information systems are part of the unification process or necessarily a result thereof but, rather, implementation of a unified system would create an administration not only sympathetic to an information system but also best able to structure and maintain one system.

Only larger municipalities can presently avail themselves (economically) of a computerized data system for evaluating correctional measures and collecting data in general. Smaller communities (or counties) must either resort to a manual system which is frequently chaotic, or worse yet, no system at all.

Processing data from a central point within the State for analysis and distribution to aid decisionmaking would be attractive, but coordinated systems may also be developed. Until unified corrections is a reality in South Dakota, administrative actions will have to suffice.

It should be noted that once the decision to proceed with unified corrections is generally accepted in this State, the entire procedure would take approximately 3 years (partly because of the constitutional amendment that will be necessary).

C. Administrative Actions:

At present, the Judiciary Department and the Board of Charities and Corrections have primary responsibility for corrections. Until corrections are unified, all systems planning must occur as a coordinated effort between these agencies. The Statistical Analysis Center (SAC) could play a role in this type of planning.

Many of the same problems faced by other criminal justice components attach here as well: shared versus dedicated computer systems, control of information (how many hands does it pass through, should it pass through), control over dissemination of data, staff loyalty (can pressure be used to force staff to allow unauthorized persons or agencies access to data?), and any of a multitude of other complications. Many of these can be worked out and handled administratively. However, when correctional functions are split among various agencies and departments, the policies followed in one agency can be different from and even work against the policies followed in other agencies. Legislation provides the basic impetus or thrust to generate interest in, and prompt development of, a corrections information system.

D. Funding:

Funding would be greatly simplified were unified corrections a reality. In the past, there has been considerable duplication of effort (pre-sentence reports being done on the same person by two different agencies, for example). Where compilation of data for management decisionmaking is concerned, such a waste of time and effort must be minimized, if not eliminated all together. Even with only probation and institutionalization/parole separated, information and decisions about an individual may be handled so that the same information is collected more than once or rehabilitation programs do not complement each other. Common record repository, hardware needs, personnel training, and reduced budget allocations are a few of the reasons supporting shared facilities and information. Federal funds could be sought for the major portion of the initial conversion/creation expenses that a unified system would require.

Standard 4.2 Uniform Classification of Data

Uniform definitions should apply to all like data in all institutions and divisions of the corrections system. Standard procedures should be established and clearly outlined for recording, collecting, and processing each item of statistical data.

Commentary

Where feasible, an individual report on each offender should be used as the basis for compiling the statistics to insure complete uniformity in coding, counting, and summarizing such data.

The records of the corrections information/statistics data must be controlled and consistent with all data coded by objective procedures.

Implementation

A. Agencies Involved:
Judiciary Department
All correctional institutions, State and local
Board of Charities and Corrections
Board of Pardons and Paroles
Attorney General's Office

B. Administrative Actions:

If nomenclature are to be standarized within any sub-system of the Criminal Justice System, an effort should be made to standarize such classifications across the system. For example, where police, courts, and corrections share common designations for criminal justice data, the problem of misinterpretation of data may be largely absent. Lack of understanding of the other components' data may result in simply ignoring the information, causing unnecessary communication gaps.

Standard 4.3 Expansion of Corrections Data Base

The corrections information/statistics system should be flexible enough to allow for expansion of the data base and to meet new information needs. A modular system should be designed and implemented to provide this flexibility. Techniques should be established for testing new modules without disrupting the ongoing operation of the system. Interaction with planners and administrators should take place before the data base is expanded or new techniques are introduced.

Commentary

The initial design of the corrections data base should take into account the fact that change is continual; therefore procedures to assure smooth transitions should be established. As new theories about variable factors are developed, new data will need to be collected to supply sufficient information for long-term research and evaluation. The time it takes for the corrections system to work means that today's programs cannot be evaluated for 3 to 5 years. Therefore, it is necessary to collect the data that will be required for analysis in 5 years.

Implementation

A. Agencies Involved:
Judiciary Department
All correctional institutions, State and local
Board of Charities and Corrections
Board of Pardons and Paroles
Also, if unified corrections is not operative, the group, committee, or agency designated to coordinate such implementation

B. Administrative Actions:

There may be some minor conflicts to be resolved where statutes that limit the kinds of data to be gathered conflict with those that attempt to expand the same data base. If the expansion involved is only qualitative expansion (increasing the likelihood of accurate data) rather than quantitative

expansion (gathering more information on more people), the conflict will be largely absent. Additionally, when expansion involves interface, for example, with the courts information system or the National Crime Information Center (NCIC), then conflicts may surface.

C. Funding:

In an effort to reduce the overall costs, system sharing may be seen as advantageous. However, when such sharing results in data overflow into other systems (e.g., police information into courts or corrections), system breeches of confidentiality may result.

Standard 4.4 Offender Statistical Data

The following types of corrections data about the offender should be collected. Minimum requirements are:

1. Official data, including date of entry into the correctional system, offenses and sentences, concurrent or consecutive sentences, recommendations of the court, conditions of work release or assignment to halfway houses or other community supervision, and county (court) of commitment or entry into the correctional system;

2. Personal data, including age, race, and sex; marital/family status; intelligence classification; military experience; classification category; other test and evaluative information, job placement, housing arrangements, and diagnostic data; and

3. Historical data, including family background, educational background, occupational record, alcohol and drug use background, and prior criminal history.

The correctional system may not need all of the information described above for persons involved in short-term custody. Each system should make a careful determination of its information needs, concerning short-term detainees.

Commentary

Standard 4.4 cites the minimum requirements for offender statistical data. This personal and historical data is necessary for effective program planning and administrative decisionmaking.

All of the types of data listed in this standard should be coded into categories that meet administrative needs and satisfy the requirments of the centralized information system.

Implementation

A. Agencies Involved:
Judiciary Department
All correctional institutions, State and local
Board of Charities and Corrections
Board of Pardons and Paroles

B. Legislation:

Because the type of information to be collected, the length of time such information may be maintained, the extent of data collected, etc., are presumably to be set forth by statute as per standards 7.2 and 7.3 infra (and section 7 generally), there must be a compromise to satisfy both standards.

Standard 4.5 Corrections Population and Movement

The corrections information and statistics system should account for the number of offenders in each corrections program and the daily changes in those numbers. Offenders should be identified by the institution or jail in which they are incarcerated or the probation, parole, or other community program to which they are assigned.

Movement of an individual from one institution or program to another should be recorded in the corrections information system as soon as possible. Assignment to special status such as work release or weekend furlough also should be recorded to enable the system to account for all persons under supervision. Sufficient information must be recorded to indentify the offender and the reason for movement. Each agency should record admissions and departures and give the reasons for each.

Commentary

The basic requirement of the corrections information system is to account for all individuals supervised by the corrections system. This is essential for institutions that submit daily movement reports detailing the inflow, outgo, and special assignment status of all individuals. Other programs such as probation or parole should not be required to submit daily reports but they should record all admissions to and departures from their programs.

With the information from these agencies, the corrections information system can update its files to reflect the current status of the corrections population.

Implementation

A. Agencies Involved:
Judiciary Department
All correctional institutions, State and local
Board of Charities and Corrections
Board of Pardons and Paroles

Standard 4.6 Corrections Experience Data

Prior to the release of the offender, data describing his corrections experiences should be added to his statistical record. When associated with postrelease outcomes, these data can be particularly valuable in evaluation correctional programs. Such data should include:

1. Summary of work and training experience, attitude, job placement, salary, etc;

2. Summary of educational experience and accomplishments;

3. Participation in counseling or other specialized programs;

4. Participation in treatment for drug addiction or alcoholism;

5. Participation in special organizations (self-help groups, civic associations);

6. Frequency of contacts with corrections staff, attempts to match offenders with corrections personnel, and direct services provided by the staff;

7. Services provided by other agencies ouside the corrections system;

8. Summary of disciplinary infractions in an institution or violations of probation or parole; and

9. Special program exposure.

Much of this information will not be applicable to persons involved in short-term custody. Each system should make an appropriate determination of its information needs concerning short-term detainees.

Commentary

In order for a complete picture of an offender to be compiled, the data listed in Standard 4.6 should be appended to his statistical record. Such information is vital to the evaluation of programs and the analysis of the relationships between corrections programs and postrelease outcomes. By using this information, each program type can finally be evaluated from the standpoint of its relevance to the successes of a client. Each program type should be held constant, with variations occurring in other data elements such as offense, age range, number of exposures to the program, and type of termination. By evaluating the programs in this manner, patterns may become apparent that may indicate the most effective types of programs for each client.

Implementation

A. Agencies Involved:
Judiciary Department
All correctional institutions, State and local
Board of Charities and Corrections
Board of Pardons and Paroles

Standard 4.7 Evaluating the Performance of the System

An information system for corrections should provide performance measures that serve as a basis for evaluation on two levels--overall performance or system reviews as measured by recidivism and other performance measures, and

program reviews that emphasize more immediate program goal achievement.

Commentary

Performance measurement is critical to evaluative program review. Standards of measurement should be uniform for external review and comparison. This requirement is especially important for fund-granting agencies, which must make decisions about program support on the basis of evaluated operational performance. Unless these measurements are based on standard criteria, reviews cannot be valid and comparisons cannot be made.

The two levels of evaluation suggested in this standard are 1) system reviews in which performance of the entire system and its goals are the object of measurement and 2) program review, in which the effectiveness of a program in achieving its objective is measured.

Implementation

A. Agencies Involved:
   Judiciary Department
   All correctional institutions, State and local
   Board of Charities and Corrections
   Board of Pardons and Paroles

Standard 5.1 Standarized Terminology

To establish appropriate communications among local, State and Federal criminal justice agencies, the data elements for identification, offense category and disposition on each offender should be consistent with specifications prescribed by the National Crime Information Center (NCIC), SEARCH Group Inc., and the Law Enforcement Assistance Administration (LEAA). There may be a need for additional or translated equivalents of the standard data elements at individual agencies; if so, it shall be the responsibility of these agencies to assure that the basic requirements of this standard are met.

Commentary

The overall purpose of Standard 5.1 is to provide the basic terminology and definitions to facilitate communication between criminal justice agencies at every level.

Both NCIC and SEARCH (System for the Electronic Analysis and Retrieval of Criminal Histories) data elements were developed by a team of criminal justice agencies working together to achieve a specific goal. Any data elements used should be dynamic and subject to future modification.

Implementation

A. Agencies Involved:
   All criminal justice agencies, State and local
   Criminal Justice Statistical Analysis Center
   SEARCH Group, Inc.

B. Administrative Actions:

Included above by virtue of the standard itself should be any Federal agencies which have data ties to State and local agencies. Suffice it to say that some agency should be designated as a clearinghouse and distribution center for purposes of insuring that all involved agencies receive and understand any changes proposed at the Federal level.

The initial program of standardization should be coordinated by or through the Statistical Analysis Center (SAC). In this way, there will exist a single, identifiable agency where all original material is readily available. There will also be a staff intimately familiar with all changes and procedures.

Standard 5.2 Programing Languages

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 controlling agency should provide the direction concerning programing language requirements already in force, or establish requirements based on the functional compatibility of language, data structure, and interface of present and potential users.

Commentary

Individual agencies at the state, county, and local levels in some instances have statutory limitations on specific programing language that may or may not be used because of the hardware in use or planned, or due to local language compatibility agreements.

There are many factors to be considered in the selection of a language, but it is to the advantage of each agency to establish such a standard at the highest possible governmental level.

The Systems Task Force feels that it is in the best interest of South Dakota to not specify a certain required language at this time. This will allow the state to establish requirements concerning program languages at a time when a computerized criminal justice system is established in South Dakota.

Implementation

A. Agencies Involved:
   All criminal justice agencies, State and local
   Criminal Justice Statistical Analysis Center

B. Administrative Actions:
   Alternatives exist in terms of designating a controlling agency. The SAC or the Attorney General's Office are two plausible choices. The decision will turn on which agency has the requisite expertise to evaluate language requirements and necessary changes. If the SAC assumes a predominate role in the entire process, as contemplated by the systems standards, its role in the above capacity will not be inconsistent.

Standard 5.3 Teleprocessing

During the design phase of the development of information and statistics systems, each agency must provide sufficient resources to assure adequate teleprocessing capability to satisfy the intra- and inter-agency communications requirements. 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 provision for interfacing with other systems as appropriate. Additionally, the specific requirements for internal communications must be included in the technical system design.

Commentary

The development of information systems tends to focus on local communications needs without considering the requirements and capabilities of other agencies with which future interfacing is essential. Communications with NCIC and the appropriate State and local systems are essential to the establishment of an effective, integrated information system to support criminal justice operations and administration.

Implementation

A. Agencies Involved:
   All criminal justice agencies, State and local
   Criminal Justice Statistical Analysis Center

B. Administrative Actions:
   The Division of Criminal Investigation is already in the position of controlling all relevant teleprocessing in South Dakota and is empowered by statute to continue doing so. The SAC should certainly give assistance in coordinating interfaces with other agencies.

OPERATIONS

Standard 6.1 OBTS/CCH Data Elements, Data Collection and File Creation

Identical data elements should be used to satisfy requirements for similar information to be developed from either an Offender-Based Transaction Statistics (OBTS) system or a Computerized Criminal History (CCH) system over all areas of South Dakota's criminal justice system.

The designs of both systems should be determined by advisory committees which should have some membership in common to assure data element compatibility. Before completion of the data element list for both systems, conferees from both advisory committees should meet to confirm data element conformity.

The coding structure of all overlapping data elements should be developed to guarantee that statistical and operational information is available, comparable, and that it meets national specifications and requirments.

The collection of data required to satisfy the OBTS and CCH systems should be gathered from South Dakota's criminal justice agencies in a single collection. Forms and procedures should be designed to deter duplication of data and assure that the data coded by agency personnel meets all of the requirements of the system.

Files created as data bases for the OBTS and CCH systems 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.

Commentary

Standard 6.1 is a thrust towards a computerized system for South Dakota. The Systems Task Force feels that many of the elements contained in Standard 6.1 should also cover a manual OBTS/CCH system.

Although the OBTS and CCH systems each have specific objectives and uses in support of criminal justice, some of the data elements are the same for both systems.

Standard 6.1 assumes that South Dakota will develop CCH and OBTS systems concurrently. If these systems are not developed simultaneously, then long range planning must be done. Such planning should insure against data and time duplication. In order for these systems to be developed logically, they should be overseen by advisory committees which are aware of the individual needs of the systems.

This type of logical planning with input from advisory committees should allow that operational data be collected in a systematic nature and that forms to collect this data be designed to insure that required data is collected and data duplication is held to a minimum.

Implementation

A. Agencies Involved:
All criminal justice agencies, State and local
Criminal Justice Statistical Analysis Center

B. Administrative Actions:
Agencies must cooperate, with the aid of the Statistical Analysis Center (SAC) as a coordinating body, in order to restructure and supplement their data gathering and reporting procedures.

C. Funding:
Federal funds are available for initiation of better data systems, but there will also be some ongoing activity above the current level for all types of agencies. Agency budgets must be adjusted so that each agency can contribute accurate, standardized information.

Standard 6.2 Establishment of Computer Interfaces for Computerized Criminal Justice Information Systems

The establishment of a computer interface to other computerized criminal justice information systems will constitute the acceptance of responsibility for a control unit for those agencies serviced by the interface.

1. Each computer interface in the criminal justice heirarchy 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 2 years--others for 1 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 logs and discrepancies between the two resolved.

Commentary

Standard 6.2 lends itself to the problems of establishing computer interfaces with other computerized criminal justice information systems. Standard 6.2 establishes the methodology that will allow agencies that cannot afford dedicated equipment to interface as long as the necessary control of the information is maintained.

This standard is futuristically oriented and is applicable only if computerized information systems are developed in South Dakota.

Implementation

A. Agencies Involved:
All criminal justice agencies participating in the criminal justice information system

B. Administrative Actions:
Because such sophisticated computer capabilities as contemplated in the standard will not become a reality in South Dakota until some time in the future, implementation is not practical at present. Without a doubt, however, careful regulation will become a necessity.

Standard 6.3 The Availability of Criminal Justice Information Systems

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 output device serving the user and may in fact be several times removed (technically) from the data base providing the information.

Commentary

The problem caused by interfacing computers from Federal to state to region to user can cause considerable system downtime while each of the individual operating centers is reporting a high degree of availability. When this reported availability is degraded by the failure of the needed repairs of any one of the technological links that connect the user to the data base, the reported reliability is significantly reduced. The standard requires that the availability of a total system (all elements) be measured at the user's device. Information centers, whether Federal, state, regional, or city, must begin to measure the availability of their systems at their output devices. This availability then will be the true measurement of the effective availability of the system.

In the past it has been the practice of the central computer complexes to report availability, measured in terms of central computers or communication computers or some other similar devices. Such computations can be misleading because information may not be available due to failures in lines, terminals, and in systems with which they are interfaced.

An index of the available data should be established and its availability measured at the user's terminal device for each functional category of data.

Once these measurements have been accomplished, efforts should be undertaken to uphold the standard of 90 percent availability for the information system.

Implementation

See Standard 6.2 supra.

PRIVACY AND SECURITY

Standard 7.1 Triggering of Data Collection

With the exception of intelligence and investigative 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.

Commentary

The requirement that criminal justice information files be triggered by an external and formal event between an individual and the criminal justice system may reduce the amount of data collected to some extent. However, it insures that the information that is retained will serve a valid purpose and be verifiable. The exception of intelligence and investigative files allows law enforcement agencies the necessary leeway to record data from informal events which may prove valuable in preventing or solving crimes.

In order to formulate standards on information, a consensus on the definitions of various types of information must be reached. Criminal histories consist of identifiable descriptions and notations of arrests, detentions, indictments, informations, or other formal criminal charges, and any disposition arising therefrom, sentencing, correctional supervision, and release. The term excludes identification information such as fingerprint records to the extent that such information does not indicate involvement of the individual in the criminal justice system. The Police Reference Notebook, published by the International Association of Chiefs of Police (IACP), defines a criminal investigation as "a police inquiry into an alleged act or omission, wherein the information obtained infers or implies the commission or an attempted commission of a crime or an offense of a criminal nature." This information gathered in the process of ascertaining the facts about and the persons responsible for crimes can be contrasted with intelligence data. The latter is collected about persons or organizations engaged in or contemplating engagement in illegal activities. While the ultimate objective of an investigation is to present physical evidence and a suspect to a court of law or to present data on an event or an individual so that decisions can be made with respect to that event or individual, the objective of intelligence gathering is to anticipate and prepare for events, either in a tactical and immediate sense or in a strategic and general sense. Either type of information may become useful for the other's purposes.

Implementation

A. Agencies Involved:

All criminal justice agencies empowered by law to collect data.

Where Grand Jury indictment or civil litigation are present, presumably without the police originating the inquiry or investigation, the courts and prosecutors' offices must particularly be included in guidelines restricting collection and maintanence of information. Courts and others may escape control by defining whatever they do as constituting investigation.

B. Legislation

Present statutes extend to fingerprints (SDCL 23-5-4), criminal records of inmates (SDCL 23-5-3), access to public records by a bureau of statistics (SDCL 23-6-11), gathering information on a particular offender (SDCL 23-6-5), and compilation of general statistical information by the Attorney General (SDCL 23-6-4). Of more importance is the fact that there is no statutory expression of when data collection will commence. SDCL 23-6-4 (Statistical Information Compilation by Director) in the final lines states that information may be gathered "for the administration of criminal justice, and for the apprehension, punishment, and treatment of criminal offenders." There is no indication that arrest need follow police contact before information may be gathered and used. In this case, it is all a matter of how liberally one construes the statute.

C. Administrative Actions:

Unless otherwise prescribed by statute, law enforcement agencies must develop their own policy designed to exclude "mere contact" individuals from becoming the subjects of police information systems.

Standard 7.2 Scope of Files

An item of data may be collected and stored in a criminal justice information system only if the potential benefits from its use outweigh the potential injury to privacy and related protected interests. Central criminal history systems should be limited to information from formal legal events.

Commentary

The less there is in a file about an individual, the less the potential for invasion of privacy. From the privacy perspective, "no file" may be the best file. Against this must be balanced the Government's right to collect and employ information about its citizens. Privacy considerations relate to the quanitity, quality, character, and intended uses of data to be collected. Since a balancing of interests is involved, from a privacy point of view, no more data collection can be justified than is essential to the performance of the criminal justice function in question. Any data collected in excess of this amount poses a potential threat to privacy without providing any offsetting benefit. All too frequently, our ability to use data effectively is exceeded by our ability to collect it. Clear definition of the purposes of data collection and its intended uses, prior to collection, would restrict acquisition to what is essential.

Thus two major questions to ask of any system are what purposes it and its data serve and how might the same purposes be accomplished without collecting these data. Further, the need for computerized files, once automation is feasible, and for permanent files should be examined carefully in light of the harm to individuals that could result from their use. Lest a concern for privacy inhibit intelligent decisionmaking by overly restricting information collection, there should be a conscious focus on gathering enough information which is pertinent to a particular case or event. Exemplifying this type of focus are the provisions of this and the previous standard to limit central criminal history systems to information from formal legal events, taken in conjunction with the standard generally mandating completeness and accuracy of records.

More specific guidelines can be drawn up by a policy-setting agency. Open disclosure and justification of each item of information and how it will be used would be one way of forcing a weighing of utility against privacy considerations. If an announcement and justification procedure were followed, adequate opportunity for receipt and assessment of public reaction could occur.

Implementation

A. Agencies Involved:

Policy-setting agency or agencies

All criminal justice agencies empowered by law to collect information and maintain files on individual citizens

B. Legislation:

The basic rationale behind involving data-collecting agencies that have a statutory basis for their activities was, first, to indicate that such activity should be restricted to only those agencies presently operating under statutory authority. Secondly, agencies collecting information by virtue of administrative policy of "general practice" should either be empowered by statute to do so or prohibited from continuing to gather information. Such constraints probably speak more to the "kind" of data and to its use than to the activities of collecting the data. Before being authorized by law to collect information, the agencies' needs for such data should be carefully scrutinized. Even if the ends are deemed worthy, lawmakers should evaluate the means of achieving such ends and decide whether data collection by those agencies is the best means. It must be made clear that authorization does not constitute permission to gather any information desired and that the criterion expressed in the standard applies to all items collected.

C. Administrative Actions:

Unless or until specified by law, all data collection by agencies not presently so authorized shall be curtailed by the supervising division. An avenue of appeal should exist to allow an agency to continue gathering data on a reduced and supervised basis. If such an agency cannot justify satisfactorily the continued collection of information or if an agency legally permitted to gather data cannot satisfactorily justify the collection of a particular item of information, that agency must be immediately restrained from continuing to collect that data by court order if necessary.

Standard 7.3 Completeness and Accuracy of Offender Data

Agencies maintaining data or files on persons designated as offenders should 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, incomplete, unclear, 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 data 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.

Criminal history items shall be destroyed from the file after one year unless the case is still pending or unless a disposition is shown.

b. 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.

When information has been purged and the individual involved is subsequently wanted or arrested for a crime, such records should be reopened 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 which has been reviewed and found inaccurate. Further, information should be purged by operations of statute, administrative regulation or ruling, or court decision, or where the information has been purged from the files of the state which originated the information.

Commentary

These guidelines recognize the need to maintain accurate and complete records and to institute formal checks insuring that the procedures established to accomplish these ends are working. Accuracy and completeness of data should improve the efficiency of criminal offender recordkeeping. However, the primary purpose is to provide a guideline for protecting security and privacy.

The file design itself can play an important role in data quality control. If one knows in advance that certain items of information may be incomplete or inaccurate, then the information should, if possible, be excluded from the system. When mistakes do occur, it is vital to notify users as soon as possible to minimize the effect that such an error might have on an individual.

For a variety of reasons, some of which are related to privacy considerations, it is sometimes desirable to remove records or remove records or entries on records from criminal justice files. Two such reasons consist of the possibilities of rehabilitation and of innocence. Since absolute rules are difficult to devise, the need for purging can be acknowledged through a general statement, while leaving decisionmaking power to the courts and agency discretion. At a minimum, the notation of an arrest not followed by a final disposition within a year should be considered incomplete if the case is not active and should be removed from an individual's record. Purging rules can become more elaborate within a particular agency as technical developments allow. Where information is removed but not destroyed, limitations on its use will guarantee that an individual is adequately protected.

Implementation

A. Agencies Involved:
All criminal justice agencies, State and local

B. Legislation:
As covered in Standard 7.1 supra, there are statutes in the area of collecting information; however, they do not restrict collection of information by various components of the criminal justice system. Similarly, there is no statutory power to guarantee accuracy, completeness, or purging with regard to the same records. Currently, juveniles enjoy the right to petition to have their records "sealed" (the relevant statute provides that only the petitioner and persons named in the petition may thereafter inspect such records, SDCL 26-8-57.1, SL 1968). For adults, SDCL 23-5-7 restricts distribution of records;

however, only one provision is made for the sealing of records at some future date. A first felony offender's records may be sealed and his or her pre-arrest status restored (SDCL 23-57-4.1, SL 1976). Statutory authority similar to that granted juveniles should be created for adults in order to conform in part with this standard.

C. Administrative Actions
Where statutory authority fails to be created, law enforcement agencies and the criminal justice system in general should seek to create a viable standardized method of dealing with inaccurate information, purging of files, and sealing records. Court order would probably be the next best method after statute, followed by an Attorney General's opinion.

Standard 7.4 Access and Dissemination.

1. General Limits on Access. Dissemination of criminal justice information will be limited to the following individuals and agencies:
Individuals and agencies which require criminal justice information to implement a statute or executive order that expressly refers to criminal conduct and contains requirements and/or exclusions based upon such conduct.

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 information should be supplied with such information only through criminal justice agencies.

3. 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 statistical portions of the file directly related to the inquiry and should maintain the anonymity of the persons involved. 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.

4. Arrest Without Conviction. If a court order is presented or upon formal notice from one criminal justice agency to another, 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. 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 South Dakota.

5. 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.

6. Currency of Information. Each criminal justice agency must ensure that the most current record is used or obtained.

Commentary

Since sensitive data will continue to be collected, its treatment while on file will determine whether a goal of confidentiality is reached. An important foundation for appropriate treatment is the granting of access only when there is an explicit legal basis. This is a formal way of identifying those agencies with a need and right to receive certain kinds of data. The need for data must be proven by demonstrating that the collection and use of that data is the best means for reaching certain goals. The right to have data must be determined by establishing the legitimacy and worth of those goals as well as whether it is that particular agency which should be achieving those goals.

In automated systems, access can be direct or indirect. To insure security and privacy it would be advisable to limit such access to the most reliable terminal users. These, presumably, would be criminal justice agencies. Non-criminal-justice agencies that are eligible to receive information would have to initiate inquiries and receive responses through criminal justice agency terminals. The slight inconvenience that this method of access imposes on non-criminal-justice users is more than offset by the increased level of control over access.

While information will vary in relevance to user requests, some data should, as a general rule, be given special attention. In particular, arrest data is potentially very damaging to an individual. The economic and personal damage resulting from an arrest that does not lead to conviction is unnecessary. The principle of presuming an individual's innocence until he is proven guilty should guide not only the criminal justice system, but other public and private systems as well. Allowing an individual to remove his/her record upon acquittal, through a court order, reflects the judgment that injurious effects would not be worth any gains for law enforcement from keeping such records and, thus, that an individual should have the opportunity to intervene and prevent such injury.

Dissemination is closely related to the problem of access. Once data is received, security and privacy considerations dictate imposition of adequate controls over its subsequent use and distribution. Dissemination to criminal justice personnel for their own use presents the fewest problems. The chief precaution to be exercised is that agency personnel have both a need and right to see the information. Within any agency, which employees may have access to what data should be specified. Each agency receiving information must enforce these standards and monitor their employees to see that they observe them. When other governmental, non-criminal-justice agencies are involved in receiving data, greater care must be exercised. Inquires, requests for data, should be satisfied only if a need and right to know are confirmed and with the minimum amount of data possible. It is virtually impossible to monitor and restrain the use of data once it passes out of the government.

There must be accountability commensurate with responsibility. Rights of access and dissemination are limited licenses to invade another person's privacy for a legitimate purpose. The user of criminal justice information must be held strictly accountable for the proper use of the information. To permit an audit of access and dissemination, it is imperative that accurate records be kept of those who received criminal justice information.

Implementation

A. Agencies Involved:

All criminal justice agencies empowered by law to collect information and maintain files on individual citizens

B. Legislation

The immense and confusing problem of defining "need to know" and "right to know" must first be dealt with by the legislature and those agencies necessarily affected. Also involved in defining the above phrases is the question of distinguishing non-criminal-justice agencies (and personnel) from quasi-criminal-justice agencies. The former have very little official contact with recognized agencies, and the latter do a substantial portion (but not all or even a majority) of their business with criminal justice agencies--schools and the Division of Motor Vehicles, respectively, are examples.

Of extant statutory authority, SDCL 23-5-1 authorizes the Office of the Attorney General to procure criminal identifying information on persons who may be taken into custody. SDCL 23-5-6 authorizes law enforcement and corrections personnel to procure identification records, and SDCL 23-5-7 prohibits the dissemination of this data outside of such agencies and prohibits its exhibition, except to peace officers. The Attorney General has the power to disseminate information held by his "bureau of statistics" to law enforcement agencies (see SDCL 23-6). There are apparently no statutory restrictions governing the extent of this and other information collected. What happens to said information if, after taken into custody, the person is released? To what uses may such data be put? Once data are gathered, the law is silent.

Restrictions presently exist in the form of opinions rendered by the Attorney General, to wit:

> Law enforcement personnel only to have access to criminal files placed in federal computer system. No. 72-63 (emphasis added);

and,

> Criminal files to be placed into federal computer system to be handled only by law enforcement personnel. No. 72-63 (emphasis added);

furthermore,

> Collection, compilation, conversion, storage and processing of criminal information may be performed only by persons under direct supervision of Attorney General. No. 72-63.

The last opinion may be interpreted to suggest that the courts and corrections agencies, unless under the Attorney General's supervision, may not collect data-- an interpretation which would not withstand even brief argument.

Of equal importance are duplicate information systems. The courts, for example, are presently developing their own system and, by virtue of SDCL 16-2-20 (SL 1973), have statutory authority to do so. A rather perplexing question for the legislators will involve guaranteeing safeguards across the criminal justice system. In other words, will agencies be able to gather information identical to a companion agency but differ as to time and method of disposing of such informations? Some agencies may be allowed to keep data on file indefinitely, while others may be required to dispose of identical data at some specified time in the future.

Other questions of a similar vein would include: to what extent and with what frequency will information exchange be allowed, if at all; will all agency personnel, by virtue of employment, have some access to data from other agencies where exchange is involved (this is particularly acute with manual systems); will one agency be able to justify maintaining data longer than another on the basis of less stringent criteria; if one agency is able to justify keeping

information almost indefinitely might it not become a "respository" for all kinds of data, some of which comparative agencies would have otherwise been forced to destroy.

C. Administrative Actions:

There is a likelihood of some conflict where statutes are not sufficiently explicit, thus forcing agencies to promulgate their own policy and procedure, which may be substantially more liberal than was the legislative intent. Policy-setting agencies such as the Attorney General's Office, the Supreme Court, and especially the Governor, could issue guidelines. Each agency must take on some additional responsibilities, such as keeping track of access and dissemination in log form, in order to demonstrate compliance with the laws or policies established.

An ongoing problem arises where sanctions must be used to curb violations by criminal justice agencies. It might, for example, be hoped that violations would be infrequent and therefore not merit undue apprehension.

D. Funding:

Where the intent is to force compliance from more recalcitrant agencies, budgets might be used in two ways. First, requested funds could be suspended until compliance with the statute, regulations, etc., is accomplished. Secondly, if consolidation of information is the ultimate goal (and this would make security much easier), then an agency's budget for data collection, storage and so forth might be reduced until compliance is the only economical way to operate. Of course, in the second instance, the system the agency has been forced to participate in must be as good (preferably better) than the system it has abandoned.

Standard 7.5 Information Review

1. Right to Review Information. Except for intelligence and investigative 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 procedures for such a review.

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. And such agency may require advance notice by the individual that he wishes to inspect his file.

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 data 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 affirmance, signed by the individual or his legal representative, that the exceptions are made in good faith and that they are true to the best of the individual's knowledge and belief.

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 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 made to the information, and should cause notice of such alterations or additions to be given to the individual involved and to any other agencies in this or any other jurisdiction to which the criminal justice information has previously been disseminated.

Commentary

A major component of the right to control the flow of information about one's self, which is one way to conceptualize the right to privacy, is the ability to review and challenge data on oneself that is held by an agency. This standard is designed to implement the right of access and is intended to achieve two complementary goals: to make the right of access reasonably and conveniently available to all citizens, and to create reasonable restrictions on the times and conditions under which the right may be exercised to assure the security of criminal offender records.

The use of a hearing officer, who is to determine whether there is prima facie evidence that criminal offender record information is inaccurate or incomplete, is intended to dispose of frivolous complaints expeditiously. The standard also provides administrative arrangements for the dissemination of notices that criminal offender record information has been found to be inaccurate or incomplete.

Implementation

A. Agencies Involved:

All criminal justice agencies that are primary information collectors (that receive or gather data for their own use and may or may not thereafter release to secondary user agencies)

B. Legislation:

Problems will doubtless arise where agencies are required to open their files to the subjects of such files. For this reason statutory force may be required to insure compliance. For example, if intelligence and investigative files are exempted, then it may be a simple matter to place almost anything into such files, knowing that the individuals involved will not be able to protest retention of such material. Granted, such actions may not be illegal per se; however, it does present some ethical problems and compromises the intent of privacy and security standards.

Review and challenging procedures are conspicuously absent from present statutes. One exception exists with regard to the recording of a convict's conduct-- the person is notified of any notation and has 30 days to challenge the entry (SDCL 24-2-17). On the other hand, parolees are forbidden to inspect their own case histories (SDCL 23-60-2), and "the public" cannot inspect identification records (SDCL 23-5-7).

C. Administrative Actions:

Standarized procedures for review would be ensured by statute; however, policy will serve well until a viable law exists. A crucial component of an agency's obilgations will be to see that corrected information reaches those who have received inaccurate data. This will serve both the individual and the agency. In the latter case, current data should benefit officials in their work and eliminate the clashes possible if changes were made in some records but not in others. These clashes could occur in court proceedings or at some other occasion where input from different sources was likely.

D. Funding:

If an individual appeals the conclusion of the agency after an audit or if information must be transferred from a central location in order that an individual may view it, a question of indigency may rightly be raised as costs may be involved. The State should bear the costs, so that review and appeal procedures are effectively available to all citizens. Otherwise, the accuracy of information collected on a given citizen may be a function of how much he/she can afford to have inaccuracies corrected.

It is not anticipated that the volume of complaints will necessitate an increment in agency budgets. Access/dissemination logs (previous standard) will permit agencies to identify other agencies to be notified of changes.

Standard 7.6 Information for Research

1. Research Design and Access to Information. Researchers who wish to use criminal justice information should submit to the agency holding the information a completed research design that guarantees adequate protection of security and privacy. Authorization to use criminal justice information should only be given when the benefits reasonably anticipated from the project outweigh the potential harm to security or privacy.

2. Limits on Criminal Justice Research. Research should preserve the anonymity of all subjects to the maximum extent possible. 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. 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 generated by the research program should be examined and verified. Data should not be released for any purposes if material errors or ommissions have occurred which would affect security and privacy.

Commentary

This standard demands that researchers respect subjects' privacy and that their projects satisfy certain security and privacy criteria as well as be supervised by the agencies whose information they analyze.

Research is a necessary function of criminal justice. Criminal justice agencies should cooperate fully with serious public and private research efforts. However, they must be alert to the potential dangers to system security and personal privacy from research programs. The researchers themselves should definitely be subject to certain minimum constraints aimed at protecting personal privacy. Standardized rules would save agencies' time and effort and help to create fairly uniform statewide practices regarding access to data.

Implementation

A. Agencies Involved:

Policy-setting agency or agencies

All agencies collecting, maintaining, or otherwise dealing with criminal justice information, whether on computer files or in a manual system

B. Administrative Actions:

Standarized policy across agencies should be promulgated by the Governor's Office in conjunction with those in charge of the various criminal justice systems. This policy should be designed to reduce the burden which would be placed on agencies to select and monitor projects, by setting forth very detailed checklists of points to look for and by designating certain people within each system who will be available to offer advice to the individual agencies. Within particular agencies, especially those of moderate to large size, certain employees could be selected and their duties expanded to include research monitoring and evaluation.

Standard 7.7 Separation of Computerized Files

For systems containing criminal offender data, the following protections should apply:

1. The computer or the portion of the computer used by the criminal justice system should be under the management control of a criminal justice agency and should be dedicated in the following manner.

a. Files should be stored in 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 update, 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 criminal justice manual or computerized files be linked to or aggregated with non-criminal-justice files for the purpose of amassing information about a specified individual or specified group of individuals.

Commentary

The specification of criminal justice management control of computerized data and of software for file protection is designed to insure that sensitive data is properly safeguarded, particularly in regard to its integrity and its use. It is important that management employ techniques appropriate to the level of the system's technology in order to satisfy the security goals set. Therefore, the standard is somewhat general in order to allow for developments in technology.

Implementation

A. Agencies Involved:

Whatever agency is ultimately vested with the responsibility of maintaining the computer system and/or the manual file system

B. Legislation:

South Dakota law does prohibit distribution of information to persons without a need or right to know. Such criteria are in need of some definition. Also, provisions should be made for offenses involving penetration into the system as outlined in the standard. Computer security is highly complex and should be augmented by statutory force.

C. Administrative Actions

A court ruling or policy would have to suffice where statutory force fails to be obtained in this area.

Standard 7.8 System Security

1. Protection from Accidental Loss. Information system operators should institute procedures for protection of information from environmental hazards including fire, flood, and power failure.

2. Intentional Damage to System. Agencies administering criminal justice information systems should adopt security procedures which limit access to information files.

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.

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 practicable, investigations should be conducted on a preemployment basis and the resulting reports used as a personnel selection device.
b. Clearance, Periodic Review, Security Manual, and In-Service Training: System personnel including terminal operators in remote locations should be assigned appropriate security clearances and should have their clearances renewed periodically after investigation and review.

Each criminal justice information system should prepare a security manual listing the rules and regulations applicable to maintenance of system 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 willfully or repeatedly to have violated the requirements of the standard (act), where other statutory provisions permit, the dissemination of criminal history record information to that agency should be prohibited for such periods and on such conditions as are deemed appropriate.

Commentary

Privacy and confidentiality of information cannot be maintained without adequate security. General areas of concern are accidents, vandalism, and unauthorized access. Since the size and facilities of agencies vary considerably throughout the state, care must be taken to adopt the standard to their needs rather than to try to formulate a uniform set of requirements. Any new systems established should incorporate security considerations in all aspects of their designs, from building construction to software procedures.

It is the human element that is most likely to provide any breach of security in the system. Procedures should be established to prevent persons posing security risks from being employed in any capacity affording them direct access to the equipment and to the records in the system. An adequate program of personnel security must cover the entire personnel process from recruitment and selection through training and discipline. This should apply to programmers, systems analysts, computer operators, terminal operators, their supervisory personnel, and other individuals involved in the preparation or dissemination of system data.

Inadequate personnel selection procedures may not show up quickly if there are serious problems in a data processing and systems organization. The only insurance against this hazard is the adoption of adequate and positive personnel selection procedures.

A security system is only as good as management's commitment to it. The managers of each information system must undertake to establish and enforce system security requirements. Senior supervisory personnel must be delegated adequate authority and responsibility to enforce security standards. Included in these standards must be sanctions adequate to inhibit accidental or intentional breaches of system security. Security breaches should be reduced through emphasis on employee knowledge of the security manual, on explanations of the rationale behind system security, and on the installation of positive attitudes toward system security in employees.

The final element in a good personnel security system is constant vigilance. System management has to be continuously on the alert for possible breaches of system discipline. Techniques such as personnel rotation, test probes, and internal security reviews of all systems and procedures by specially assigned personnel would help to maintain the integrity of the system.

Implementation

A. Agencies Involved:
Policy-setting agency or agencies
All agencies maintaining criminal justice information, whether on computer files or in a manual system

B. Administrative Actions
Rules and policy pertinent to screening, review, etc., should be standarized in order to prevent each agency from creating very distinct rules and procedures. Highly individualized rules will only add to the confusion. Guidelines should be issued by the Attorney General or whoever has been vested with the responsibility for seeing that records are kept private and secure. As for all other standards in this sphere, all segments of the criminal justice system are covered. Thus cooperation between law enforcement, the courts, and corrections is crucial if concepts such as security are to become a practical reality. Lax security in one area, to the extent that data is shared, undermines security in the other areas. The Governor should exert leadership and encourage coordination.

Additionally, consideration should be given to setting forth sanctions in statutory form, if for no other reason, so that due process will protect the innocent.

C. Funding:
Several avenues exist for funding. The State could assume responsibility for providing security manuals and other aid, perhaps by appointing a privacy and security officer. The legislature could appropriate funds to be dispensed through the State Criminal Justice Commission and the District Criminal Justice Commissions, or through some other agency, or to be given to the groups in charge of the separate information systems established. To the extent that individual

agencies must institute procedures or purchase equipment in order to comply with statute or policy, the necessary increases in their budgets should be automatically granted.

Standard 7.9 Security and Privacy Administration

1. South Dakota should amend present legislation for protection of security and privacy in criminal justice information systems. The amended statutes shall establish minimum standards for protection of security and privacy, and civil and criminal sanctions for violations of statutes or rules and regulations adopted. Penalities should apply to improper collection, storage, access, and dissemination of criminal justice information.

2. Training of System Personnel. All persons involved in the direct operation of a criminal justice information system should be required to attend approved courses of instruction concerning the system's proper use and control. Instruction may be offered by any agency or facility, provided that curriculum, materials, and instructors' qualifications have been reviewed and approved. Each operator or supervisor shall attend a course of instruction within a reasonable period of time after assignment to the criminal justice information system.

Commentary

South Dakota has enacted some legislation relevant to privacy and security; these laws must be updated and expanded to confront current and potential problems. Police guidelines are needed if a balance between agency responsibilities and privacy protection is to be struck, and these must be more extensive and adaptable than legislation.

A variety of sanctions should be available, up to and including removal of an agency from statewide information networks and prohibition against dissemination of criminal justice information to offending agencies. Individual offending employees should be disciplined by their own agencies. In addition to civil and criminal penalties for breaches of security and privacy, agencies should punish such employees by suspension, reduction in grade, transfer, discharge, or other administrative penalties. Failure to exercise adequate control over its employees should be grounds for sanctions against the agency itself.

Implementation:

A. Agencies Involved:
Policy-setting agency or agencies
Legislative Research Council
Agencies capable of rendering technical and training assistance (e.g., Criminal Justice Statistical Analysis Center and Division of Criminal Investigation)

B. Legislation:
Sanctions for misuse of data should be set forth statutorily in order that legal action may be initiated by, for example, local law enforcement or other criminal justice personnel who may witness or are party to illegal handling of sensitive information.

C. Administrative Actions:
Barring existence of statutory force, policy should be created to support similar safeguards. Such policy may be authored by the Attorney General

or the Office of the Governor. Even where legislation exists, guidelines should cover those areas which are not explicit enough in the legislation or for which legislation is not appropriate. In any event, policies regarding training must be articulated. The Attorney General or the Governor could define training requirements to be satisfied through an existing agency such as the Division of Criminal Investigation, through programs set up at large criminal justice agencies, and/or through periodic special workshops or seminars. Each agency would be expected to adequately train its own personnel for its own individual information system, to the extent that the system differs from those of other similar agencies or to the extent that individual agencies must assume responsibility for training in the absence of statewide programs.

D. Funding:

Training money could be granted directly to the agency or agencies offering the instruction; it could be derived from supervisory agencies' budgets; it could be allocated by the legislature as training funding to be administered by some existing agency. Where possible, employees should participate in common training programs to cut down duplication of training efforts on the local level and to minimize the need for any increase in local budgets for training purposes.

DCI has been designated as the official agency for training law enforcement officers (SDCL 23-3-18), and a standards commission has broad powers with regard to training (SDCL 23-3-35). The mode(s) of funding will depend on the type of coordination established among law enforcement, courts, and corrections agencies. For example, if DCI were charged with all systems personnel training, one budgetary increase could suffice.

STRATEGY FOR IMPLEMENTING STANDARDS

Standard 8.1 The Establishment of Criminal Justice Information Systems User Groups

Each multi-agency criminal justice information system should establish a user group representing the agencies who receive or provide the information services. These groups should have influence over the operation and development of the system.

Commentary

A properly constituted user group is important in that its advice is needed to minimize duplication and enhance cooperation between the agencies that comprise South Dakota's Criminal Justice System. This proposed user group should be small enough to serve as a contributor in the development of the system and also to become an involved partner in the final operating system.

Implementation

A. Agencies Involved:
All criminal justice agencies, State and local, and their representatives
Criminal Justice Statistical Analysis Center

B. Administrative Actions:

The Division of Criminal Investigation, the Courts, and Correctional agencies each possess some form of a criminal justice information bank. These agencies are in a position to be aware of the many pitfalls that may arise. Because the major types of agencies involved are few, coordination should be a relatively easy matter.

Standard 8.2 System Planning

South Dakota should establish a specific plan for the feasibility of and the development of information and statistical systems at State and local levels. Critical elements of the plan are as follows:

1. The plan should specify system objectives and services to be provided, including:
a. Jurisdictional (State, local) responsibilities;
b. Organizational responsibilities at the State level;
c. Scope of each system; and
d. Priorities for development.

2. The plan should indicate the appropriate funding source both for development and operation of the various systems.

3. The plan should provide mechanisms for obtaining user acceptance and involvement.

Commentary

South Dakota needs a specific system plan to identify objectives and services, especially those specified in the standard. No plan will succeed without adequate funding and the cooperation and enthusiasm of the user agencies.

This plan should serve as a guideline for system development as well as to document the feasibility of the components of the system in relation to a state such as South Dakota.

Implementation

A. Agencies Involved:
   All criminal justice agencies, State and local
   State Criminal Justice Commission
   District Criminal Justice Commissions
   Criminal Justice Statistical Analysis Center
B. Administrative Actions:

South Dakota presently has no plan which would serve as a detailed guide to systems design; therefore, the Governor might profitably appoint an agency to lead such a committee, commission, or task force to study the problem in depth. This kind of arrangement might allow input from groups and individuals such as the Statistical Analysis Center (SAC).

Whatever is developed will not, of course, be the final answer; part of the standard covers areas such as jurisdiction and funding. It may, therefore, be necessary to pursue legislation in order to establish such a plan (and its updates) as a permanent part of the State Criminal Justice System.

Standard 8.3 Systems Analysis and Design

Any individual systems covered under the plan described above, funded by monies from the Omnibus Crime Control and Safe Streets Act of 1968 or other State grant programs, should be predicated on a system analysis and design consistent with the standards in this report.

Commentary

General conformity with the standards developed by this Task Force should be considered in grant approval in State programs involving Safe Streets Act money and other funding sources. This conformity may also be considered in system designs funded by local sources. Instant conformity is not expected but progress towards that end is recommended.

Implementation:

A. Agencies Involved:
   All criminal justice agencies, State and local
   Division of Law Enforcement Assistance
B. Funding:

Guidelines for funding arrangements should be compiled, disbursed, and explained by the Division of Law Enforcement Assistance (DLEA) staff. Evaluation of program possibility (or redesign, for systems already operational) should remain with the agencies as a group or that agency designated as in control. For unbiased evaluation, the SAC may be of considerable assistance.

EVALUATION STRATEGY

Standard 9.1 Preimplementation Monitoring

Preimplementation monitoring should consist of a continuous review, analysis, and assessment of available documentation and milestone achievement covering system analysis, design, development, and initial steps leading toward actual implementation. All items should be monitored relative to costs (both dollars and man-hours); milestone accomplishment (time); and quality (response time, scope, sophistication, and accuracy). Both intra-and inter-agency considerations should be included, particularly with respect to consistency with other planned or operational information and statistical systems.

Where feasible and appropriate the following items should be considered in this monitoring standard:

1. *System Analysis Documentation*

2. *System Recruitment Documentation*

3. *System Design Documentation*
   a. *Functional specifications;*
   b. *Component flow charts;*
   c. *Data base design (or administration);*
   d. *Groupings of files;*
   e. *Structure of data in files;*
   f. *File maintenance;*
   g. *File capacity;*
   h. *Timeliness of data inputs to files;*
   i. *Data standards;*
   j. *Module interfaces/data links;*
   k. *Edit criteria;*
   l. *Output reports; and*
   m. *Response time requirements.*

4. *System Development Documentation*
   a. *Module description;*
   b. *Component description;*
   c. *User manuals;*
   d. *Operations description;*
   e. *Data base description; and*
   f. *Processing modes description (manual, computer-based batch, on-line, real-time).*

5. *System Implementation Documentation*
   a. *Component implementation report;*
   b. *Data base implementation report;*
   c. *Test plan report;*
   d. *Hardware requirements report;*
   e. *Software requirements report;*
   f. *Physical site report;*
   g. *Data security and confidentiality report;*
   h. *Implementation monitoring report;*
   i. *Impact evaluation report; and*
   j. *System training report.*

Commentary

Preimplementation monitoring is concerned with the effectiveness of the design of the proposed system, not only with respect to potential users of the system but also relative to other systems and agencies. The preimplementation monitoring and documentation make extensive use of prior, related, successful system development.

Implementation

A. Agencies Involved:
All user agencies involved in the Criminal Justice Information System
Criminal Justice Statistical Analysis Center

B. Administrative Actions:
The difficulty of drafting an applicable statute necessitates deferring to administrative policies. All relevant agencies should be involved from the beginning, and by consensus of the others, an agency may be designated as a clearinghousefor questions, problems, and dissemination of successful strategies to other user agencies.

Whether or not the Statistical Analysis Center (SAC) is in the most advantageous position to accomplish these ends may be debatable. There is no question, however, that the SAC has both the requisite expertise and time to devote to such an undertaking.

C. Funding:
Funding may have to be restricted to each agency's budget with supplemental assistance from the Law Enforcement Assistance Administration (LEAA). The initial development comprises most of the work and once the system is operating, standarized procedures will enable each user agency to monitor on an in-house basis.

Standard 9.2 Implementation Monitoring

A key consideration in implementing systems is providing maximum assurance that the eventual operating system meets the design objectives. Implementation monitoring should employ a specific series of quantifiable measuring instruments that report on the cost and performance of component parts and the total system. The cost/performance monitoring of an operating or recently developed system should focus on: man-machine interaction, software (computer and/or manual processes), and hardware (computer and/or non-automated equipment).

Commentary

The component and total system cost is not just the one-time development and implementation cost, but it also includes recurring annual operating costs.

Although this aspect of evaluation is relatively novel, it is important if any consistency of measurement of effectiveness of the system is to be achieved.

Implementation

A. Agencies Involved:
All criminal justice agencies, State and local with emphasis on the agencies in control of the component information systems

B. Administrative Actions:
The same comments found in section B of Standard 9.1 apply here.

C. Funding:
There is some question as to whether or not such a procedure might not be better implemented via legislation in order to provide a constant source of funding; such a decision must ultimately rest with those agencies involved.

Standard 9.3 Impact Evaluation

Periodic impact evaluation of the entire South Dakota Criminal Justice Information System should be conducted as appropriate and feasible.

Periodically, or upon request by the Information Systems Advisory Committee to the South Dakota Criminal Justice Commission, the system's component agencies shall design and implement a systematic procedure for impact evaluation which should determine:

1. What information, communication, and decision processes in a criminal justice agency exhibit the greatest positive and negative impact due to the information and statistical system;

2. What relationships exist between specific features of the system and the benefits to the user; and

3. Attitudinal and behavioral changes produced by the information systems.

Commentary

This standard states that impact evaluation should determine 1) what information, communication, and decision processes exhibit the greatest positive and negative impact due to the information system; and 2) what relationships exist between specific features of the system and the benefits to the user. On paper these targets for evaluation seem dictated by common sense and perhaps best suited to informal inquiry. But, due to a lack of experience in the area of evaluation of information systems, even formal methods of evaluation are often vague, untested, or both. To gain the most from an information system, evaluations should be conducted in the most thorough and conclusive manner possible. The attitudinal and behavioral effects of information systems are usually not taken into account, yet they have a major impact on how the system is used and how it in turn affects agency operations.

The development of a strategy to evaluate the impact of the criminal justice information system is going to be a complex task since the agencies involved already have a difficult time evaluating their own successes. The relationship of an information system to an agency's operational effectiveness is often clouded by the contribution of the decisionmaking mechanisms which the information systems are supposed to assist.

The implementation of a formal evaluation program does provide some assurance against premature judgments of costs and benefits. Furthermore, the development of evaluation models and strategies will contribute to a better understanding of the overall criminal justice information system. The success of the evaluation program depends not only on a carefully constructed program, but also on the preparation called for through preimplementation and implementation monitoring.

Implementation

A. Agencies Involved:
All criminal justice agencies, State and local
State Criminal Justice Commission
Criminal Justice Statistical Analysis Center

B. Administration Actions:
Such a plan of evaluation will require considerable coordination either through the SAC or some other designated agency. Since the SAC's position is that of receiving input from all criminal justice agencies across the State, the task of evaluation could be simplified by using the SAC. Problems may arise where another agency is designated to perform the impact evaluation; State agencies are frequently in competition with each other (budgets, personnel, etc.) and this condition may lead to a situation that is best avoided, if possible. The SAC should have no vested interests that would result in intentional misinterpretation of data.

C. Funding:
A combination of State, county, and local funding, coupled with LEAA grants, may be most appropriate.

END