

58873

*Developed standards  
for information systems  
a year ago.*



**ILLINOIS LAW ENFORCEMENT COMMISSION**

120 SOUTH RIVERSIDE PLAZA  
CHICAGO, ILLINOIS 60606  
312/454-1560

*1977*

**standards:**

---

**Criminal**

**Justice**

**Information**

**Systems**

*58873*

*IL  
.005*

## Standard 1.1 - CRIME-ORIENTED PLANNING

Every criminal justice planning agency and coordinating council should:

1. Analyze the crime problems in its jurisdiction;
2. Identify specific crimes deserving priority attention;
3. Establish quantifiable and time phased goals for the reduction of priority crimes;
4. Evaluate and select alternative strategies and programs for reducing priority crimes;
5. Allocate its own funds and staff resources in accordance with the crime goals, strategies, and programs chosen;
6. Maintain close working relationships with criminal justice and other public agencies to implement crime reduction goals and objectives; and
7. Assume responsibility for the effective evaluation of its planning and funding decisions, and the use of evaluation results to refine goals, strategies, and programs.

## Standard 1.2 - IMPROVING THE LINKAGE BETWEEN PLANNING AND BUDGETING

State and local governments in Illinois should develop mechanisms for introducing the analyses and recommendations of criminal justice planning agencies into their budgetary processes. These mechanisms may include formal integration of planning and budgeting efforts through program budgeting systems, the institution of planning and budgeting staff coordination procedures, and the development of detailed master plans for specific areas of criminal justice operations.

1. By 1978, the ILEC should develop a general system of multiyear planning that takes into account all funds directed to crime control activities within the State. This would include all sources of Federal funds; State, general, and capital funds; and private donations, endorsements, and contributions. Where available, the relevant State program budgeting format should be employed. Substate criminal justice planning agencies and councils should establish congruent and supportive systems of multiyear planning to those established by the State.

2. Planning and budgeting units should immediately adopt additional coordinating mechanisms such as joint staff teams on special problems and planning staff participation budget hearings.

3. Detailed "master plans" should be developed where appropriate for those specific areas of criminal justice operations that require forecasts of long-term problems and needs. Assuming continuous evaluation and update, such plans should serve as a basis for annual budgeting and appropriations decisions. Although either operating agencies or criminal justice planning agencies may provide and direct staff effort, both should be directly involved in the development of master plans.

#### Standard 1.3 - SETTING MINIMUM STATEWIDE STANDARDS FOR RECIPIENTS OF GRANTS AND SUBGRANTS

The ILEC should establish minimum standards for making grants and subgrants from all funds under its control to criminal justice and related public and private agencies. Grants and subgrants to specific agencies should be contingent upon the agency's adoption of established minimum standards.

1. Standard-setting efforts should be limited to those human resources, physical resources, and management and operations requirements that are clearly essential to the achievement of the goals of the criminal justice system.

2. Where existing State bodies have established standards, such standards should be considered controlling, and the ILEC should use them as minimum standards for funding.

3. Standards should be adopted by the ILEC only after a thorough effort has been made to notify all interested and affected parties and to solicit their opinions.

4. The ILEC in its standard setting efforts should refer to, and consider, major national studies on standards, such as the National Advisory Commission on Criminal Justice Standards and Goals, and the standards of major professional associations.

5. Continuous evaluation of the usefulness of adopted standards in meeting established goals should be undertaken by the ILEC.

### Standard 3.1 - COORDINATION OF INFORMATION SYSTEMS DEVELOPMENT

Illinois 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 that will satisfy information needs of management decision making 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.

### Standard 3.2 - STATE ROLE IN CRIMINAL JUSTICE INFORMATION AND STATISTICS

Illinois 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 the Secretary of State;

4. A high-speed interface with NCIC providing access to all NCIC files as consistent with Illinois privacy and security regulations, where they are at variance with NCIC regulations;

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 (formatting) 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 files as consistent with Illinois privacy and security regulations, where they are at variance with NCIC regulations.

10. Reporting offender-based transaction statistics to the Federal Government.

### Standard 3.3 - LOCAL CRIMINAL JUSTICE INFORMATION SYSTEMS

Every locality should be serviced by a local\* criminal justice information system which supports the needs of criminal justice agencies.

\*"Local" as used in this and following standards means a criminal justice information system serving one or more governmental subdivisions below the State level. Multi-jurisdictional (i. e., "regional") criminal justice information systems fall within the definition of a LCJIS. (See Standard 10.4)

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 the present criminal justice status for each individual under the cognizance of criminal justice agencies within that locality.

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

4. 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.

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

6. 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.

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

#### Standard 3.4 - 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.

#### Standard 4.1 - 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 followup 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.

#### Standard 4.2 - CRIME ANALYSIS CAPABILITY

Every police department should improve its crime analysis capability by utilizing information provided by its information system and by the State and regional information systems. 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.

#### Standard 4.3 - MANPOWER RESOURCE ALLOCATION AND CONTROL

Every police agency should develop a manpower resource allocation and control system that will support major efforts to:

1. Identify through empirical means the need for manpower within the department;
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 the adopted plan.

#### Standard 4.4 - 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.

#### Standard 4.5 - UCR PARTICIPATION

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

#### Standard 4.6 - 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, including coded geographical location and type of 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.

#### Standard 4.7 - QUALITY CONTROL OF CRIME DATA

Every police agency should make provision for an independent 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.

To establish an "audit trail" and to provide the basic documentation needed by management, the following key characteristics or records should be adopted:

1. The police response made to every call for police service should be recorded, regardless of whether a unit is dispatched. Dispatch records should be numbered and time noted; if the service leads to a complaint, the complaint should be registered on a numbered crime report, and that number also be shown on the dispatch record.

2. All dispatches should be recorded, indicating time of dispatch and arrival on scene.

3. Dispatch records should show the field unit disposition of the event, and should be numbered in such a way as to link dispatches to arrest reports or other event disposition reports.

4. All self-initiated calls should be recorded in the same manner as citizen calls for service.

#### Standard 4.8 - GEOCODING

Where practical, and in concert with Illinois Criminal Justice Information System requirements, 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.

## Standard 5.1 - DECISION MAKING IN INDIVIDUAL CASES

A court information system should provide information unique to the defendant and to the case, such as the following:

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), representation, and other participants.

## Standard 5.2 - CALENDAR MANAGEMENT IN THE COURTS

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 attorney and police witness schedule which can be used to minimize scheduling conflicts;
3. Judge and courtroom schedule;
4. Range of time which proceedings consume;
5. An age index of all cases in pretrial or awaiting trial (by type of trial requested) to determine if special attention is required or the speedy trial rule endangered;
6. An index relating scheduled cases to whether the defendant is confined, released, rearrested, at large, or undergoing adjudication on a separate offense;
7. An index of multiple cases pending against individual defendants, to permit consolidation;

8. An index of information on possible or existing case consolidations; and

9. An index of defendants whose existing probation or parole status may be affected by the outcome of current court action.

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

#### Standard 5.3 - COURT MANAGEMENT DATA

For effective court administration, 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 dispositions -- number of cases filed and the number of defendants disposed of by offense categories;

2. Monthly inventory -- cases in pretrial or preliminary hearing stage; cases scheduled for trial (by type of trial) or preliminary hearing; and cases scheduled 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;

6. Prosecutor/defense counsel workload -- number of cases disposed of by type of disposition and type of proceeding or calendar according to prosecutor, appointed defense counsel, or private defense counsel representation;

7. Jury utilization -- number of individuals called, placed on panels, excused, and seated;

8. Number of defendants admitted to bail, released on their own recognizance, or retained in custody;

9. Number of witnesses called at hearings on serious felonies, other felonies, and misdemeanors; and

10. Courtroom utilization record.

#### Standard 5.4 - 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. A means of weighting cases according to prosecution priority, policy, and the probability of success;
2. Time periods between major steps in adjudication;
3. Daily calendar workloads and dispositions;
4. 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;
5. Case schedule index listing police witnesses, expert witnesses, defense counsel, assigned prosecutor, and type of hearing.
6. Record of continuances by case, number, and party requesting;
7. Selection criteria for witnesses at court hearings.

#### Standard 5.5 - 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.



## Standard 6.1 - DEVELOPMENT OF A CORRECTIONS (INCLUDING PROBATION) 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.

## Standard 6.2 - 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.

## Standard 6.3 - EXPANSION OF CORRECTIONS

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.

#### Standard 6.4 - 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; military experience; classification category; other test and evaluative information, job placement, housing arrangements, and diagnostic data; and
3. Historical data, including family data, educational data, occupational record, alcohol and drug use data, 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.

#### Standard 6.5 - 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 identify the offender and the reason for movement. Each agency should record admissions and departures and give the reasons for each.

#### Standard 6.6 - 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 evaluating correctional programs. Such data should include:

1. Summary of work and training experience, 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, community-based programs);
6. Frequency of contacts with major programs, attempts to match offenders with directors of major programs, and direct services provided by the programs;
7. Services provided by other agencies outside 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.

#### Standard 6.7 - EVALUATION 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.

Standard 7.1 - DATA ELEMENTS FOR OFFENDER-BASED TRANSACTION  
STATISTICS AND COMPUTERIZED CRIMINAL HISTORY  
RECORDS

Identical data elements should be used to satisfy requirements for similar information to be developed from either an OBTS or CCH system over all areas of the criminal justice system.

Advisory committees determining the designs of both systems should have some membership in common to assure data elements 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 both statistical and operational information will be available and comparable. Where national specifications and requirements for data element structure exist, they should be considered the minimum acceptable.

Standard 7.2 - CRIMINAL JUSTICE AGENCY COLLECTION OF OBTS-CCH  
DATA

The collection of data required to satisfy both the OBTS and CCH systems should be gathered from operating criminal justice agencies in a single collection and be maintained in one place. Forms and procedures should be designed to assure that data coded by agency personnel meets all requirements of the information and statistics systems, and that no duplication of data is requested.

Standard 7.3 - OBTS-CCH FILE CREATION

Files created as data bases for OBTS and CCH systems, because of their common data elements and their common data input from operating agencies, should be developed simultaneously and maintained as much as possible within a single activity.

Juvenile record information should not be entered into adult criminal history files or adult OBTS files.

#### Standard 7.4 - TRIGGERING OF DATA COLLECTION

With the exception of intelligence files, collection of criminal justice information concerning individuals should be triggered only by a formal event in the criminal justice process and contain only verifiable data. In any case where dissemination beyond the originating agency is possible, this standard should be inviolable.

#### Standard 7.5 - COMPLETENESS AND ACCURACY OF OFFENDER DATA

Agencies maintaining data or files on persons designated as offenders shall establish methods and procedures to insure the completeness and accuracy of data, including the following:

1. Every item of information should be checked for accuracy and completeness before entry into the system. In no event should inaccurate, 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. In no event should information about cases still pending be disseminated without information indicating the current case status.

3. Unless otherwise required by Illinois law, the following rules shall apply to purging these records:

- a. General file purging criteria. In addition to inaccurate, incomplete, misleading, unverified, and unverifiable items of information, information that, because of its age or for other reasons, is likely to be an unreliable guide to the subject's present attitudes or behavior should be purged from the system. Files shall be reviewed periodically.

b. Purging by virtue of lapse of time. Every copy of criminal justice information concerning individuals convicted of a serious crime should be purged from active files 10 years after the date of release from supervision. In the case of less serious offenses the period should be 5 years. Information should be retained where the individual has been convicted of another criminal offense within the United States, where he is currently under indictment or the subject of an arrest warrant by a U.S. criminal justice agency.

c. Use of purged information. Information that is purged but not returned or destroyed should be held in confidence and should not be made available for review or dissemination by an individual or agency except as follows:

(1) Where necessary for in-house custodial activities of the recordkeeping agency or for the regulatory responsibilities of the Illinois Criminal Justice Information Systems Board;

(2) Where the information is to be used for statistical compilations or research studies, in which the individual's identity is not disclosed and from which it is not ascertainable;

(3) Where the individual to whom the information relates seeks to exercise rights of access and review of files pertaining to him;

(4) Where necessary to permit the adjudication of any claim by the individual to whom the information relates that it is misleading, inaccurate, or incomplete; or

(5) Where a statute of a State necessitates inquiry into criminal offender record information beyond the 5- and 10-year limitations.

When the information has been purged and the individual involved 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 about which a challenge has been upheld. Further, information should be purged by operation 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.

#### Standard 7.6 - SEPARATION OF COMPUTERIZED FILES

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

1. At the State level all criminal offender record information should be stored in a computer dedicated solely to and controlled by criminal justice agencies.

2. At the regional or local level, where limitations prevent the use of a solely dedicated computer, that portion of the computer and associated peripheral devices used by the criminal justice system should be under the management control of a criminal justice agency in the following manner:

- a. Files should be stored on the computer in such a manner that they cannot be modified, destroyed, accessed, changed, purged, or overlaid in any fashion by non-criminal-justice terminals.

- b. The senior criminal justice agency employee in charge of computer operations should write and install, or cause to have written and installed, a program that will prohibit inquiry, and record updates or destruction of records from any terminal other than criminal justice system terminals which are so designated.

The destruction of records should be limited to specifically designated terminals under the direct control of the criminal justice agency responsible for maintaining the files.

c. The senior criminal justice agency employee in charge of computer operations should have written and installed a classified program to detect and store for classified output all attempts to penetrate any criminal offender record information system, program, or file.

This program should be known only to the senior criminal justice agency employee, 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.

d. The appropriate criminal justice agency or agencies should obtain assurances of the necessary reliability and availability of the system, or system services they will use, by contractual arrangements.

3. 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.

#### Standard 7.7 - ESTABLISHMENT OF COMPUTER INTERFACES FOR CRIMINAL JUSTICE INFORMATION SYSTEMS

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

1. Each computer interface in the criminal justice hierarchy from local criminal justice information systems through the national systems will be considered a control terminal and allowed to interface if all of the identified responsibilities are accepted by that control unit.

2. Each control unit must maintain technical logging procedures and allow for 100 percent audit of all traffic handled by the interface. Criminal history response logs should be maintained for 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.

#### Standard 7.8 - THE AVAILABILITY OF CRIMINAL JUSTICE INFORMATION SYSTEMS

The availability of an automated information system 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.

For an on-line system, availability is the ratio of the time that the system is fully operating and can process inquiries to the time that it should be available.

For a batch process system, it is the percentage of the time it is processing jobs on schedule, according to a schedule predetermined by the user and the computing facility management.

## Standard 8.1 - SECURITY AND PRIVACY ADMINISTRATION

1. State Enabling Act. The State of Illinois should adopt enabling legislation for protection of security and privacy in criminal justice information systems. The enabling statute shall establish an administrative structure, minimum standards for protection of security and privacy, and civil and criminal sanction for violation of statutes or rules and regulations adopted under it.

2. Illinois Criminal Justice Information Systems Board (ICJISB). Illinois shall establish - by legislative act - a Criminal Justice Information Systems Board. Not less than one third of the members named to the Board shall be private citizens who are unaffiliated with the State's criminal justice system. The remainder shall include representatives of the criminal justice information systems and other appropriate government agencies. The ICJISB shall be vested with sufficient authority to adopt and administer security and privacy standards for all criminal justice information systems within Illinois and to establish the operating policies of the State CJIS.

Civil and criminal sanctions should be set forth in the enabling act for violation of the provision of the statute or rules or regulations adopted under it. Penalties should apply to improper collection, storage, access, and dissemination of criminal justice information.

3. Training of System Personnel and Public Education. All persons involved in the direct operation of an automated 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 by the Board.

Minimum course time should be 10 hours for operators, with 15 hours required of immediate supervisors. Each operator or supervisor shall attend a course of instruction within a reasonable period of time after assignment to the criminal justice information system.

The Board should conduct a program of public education concerning the purposes, proper use, and control of criminal justice information. It may make available upon request facilities, materials, and personnel to educate the public about the purposes, proper use, and control of criminal justice information.

## Standard 8.2 - 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.

## Standard 8.3 - ACCESS AND DISSEMINATION

Unless otherwise required by Illinois law:

1. General Limits on Access. Information in criminal justice files should be made available only to public agencies which have both a "need to know" and a "right to know". The user agency should demonstrate, in advance, that access to such information will serve a criminal justice purpose.

2. Terminal Access. Criminal justice agencies should be permitted to have terminal access to computerized criminal justice information systems where they have both a need and a right to know. Non-criminal justice agencies having a need and right to know or being authorized by statute to receive criminal justice information should be supplied with such information only through the State CJIS under regulations set forth by the ICJISB.

3. Certification of Non-Criminal-Justice Users. ICJISB should receive and review applications from non-criminal-justice government agencies for access to criminal justice information. Each agency which has, by statute, a right to such information or demonstrates a need to know and a right to know in furtherance of a criminal justice purpose should be certified as having access to such information through the State CJIS.

4. Limited Access to Data. Criminal justice agencies should be entitled to all unpurged data concerning an individual contained in a criminal justice information system only on a need to know basis. Non-criminal-justice agencies should receive only those portions of the file directly related to the inquiry. Special precautions should be taken to control dissemination to non-criminal-justice agencies of information which might compromise personal privacy including strict enforcement of need to know and right to know criteria.

5. Arrest Without Conviction. All copies of information filed as a result of an arrest that is legally terminated in favor of the arrested individual should be expunged and returned to that individual within 60 days of final disposition and purged from automated systems, or if a court order is presented, or upon formal notice from one criminal justice agency to another. Information includes fingerprints and photographs. Such information should not be disseminated outside criminal justice agencies.

However, files may be retained if another criminal action or proceeding is pending against the arrested individual, or if he has previously been convicted in any jurisdiction in the United States of an offense that would be deemed a crime in Illinois, or if he is a fugitive, unless expungement is ordered by a court.

6. Dissemination. Dissemination of personal criminal justice information should be on a need and right to know basis within the government. There should be neither direct nor indirect dissemination of such information to nongovernmental agencies or personnel. Each receiving agency should restrict internal dissemination to those employees with both a need and right to know.

Legislation should be enacted which limits questions about arrests on applications for employment, licenses, and other civil rights and privileges to those arrests where records have not been returned to the arrested individual or purged. Nor shall employers be entitled to know about offenses that have been expunged by virtue of lapse of time.

7. Accountability for Receipt, Use, and Dissemination of Data. Each person and agency that obtains access to criminal justice information should be subject to civil, criminal, and administrative penalties for the willful improper receipt, use, and dissemination of such information.

The penalties imposed would be those generally applicable to breaches of system rules and regulations as noted earlier.

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

## Standard 8.4 - CRIMINAL HISTORY RECORD INFORMATION REVIEW

1. Right to Review Information. Every person should have the right to review criminal history record information relating to him. Each criminal justice agency with custody or control of criminal history record information shall make available convenient facilities and personnel necessary to permit such reviews. Criminal history records are those records kept by agencies to summarize the experience of an individual with that agency or with the criminal justice system, whether they are automated or manual records.

### 2. Review Procedures.

a. Any individual who believes that a criminal justice information system or criminal justice agency maintains criminal history record information concerning him, shall upon satisfactory verification of his identity, be entitled to review such information in person or through counsel and to obtain a certified copy of it for the purpose of challenge or correction.

b. 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 history record information he has reviewed. The form should include a recording of the name of the reviewing individual, the date of the review, and whether or not any exception was taken to the accuracy, completeness, or contents of the information reviewed.

c. 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 form should include an affirmation, 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. One copy of the form shall be forwarded to the Illinois CJIS Board.

d. The criminal justice agency should in each case conduct an audit of the individual's criminal history record information to determine the accuracy of the exceptions. The ICJISB and the individual should be informed in writing of the results of the audit. Should the audit disclose inaccuracies or omissions in the information, the criminal justice agency should cause appropriate alterations or additions to be made to the information, and should cause notice of such alterations or additions to be given to the Board, the individual involved, and any other agencies in this or any other jurisdiction to which the criminal history record information has previously been disseminated.

### 3. Challenges to Information.

a. Any person who believes that criminal history record information that refers to him is inaccurate, incomplete, or misleading may request any criminal justice agency with custody or control of the information to purge, delete, modify, or supplement that information. Should the agency decline to do so, or should the individual believe the agency's decision to be otherwise unsatisfactory, the individual may request review by the ICJISB.

b. Such requests to the Board (in writing) should include a concise statement of the alleged deficiencies of the criminal history record information, shall state the date and result of any review by the criminal justice agency, and shall append a sworn verification of the facts alleged in the request signed by the individual or his attorney.

c. The Board should establish a review procedure for such appeals that incorporates appropriate assurances of due process for the individual.

## Standard 8.5 - DATA SENSITIVITY CLASSIFICATION

1. Each criminal justice agency maintaining criminal justice information should establish procedures in order to implement a sensitivity classification system. The general guidelines for this purpose are:

- a. Places and things should be assigned the lowest classification consistent with their proper protection.
- b. Appropriate utilization of classified places and things by qualified users should be encouraged.
- c. Whenever the sensitivity of places or things diminishes or increases it should be reclassified without delay.
- d. In the event that any place or thing previously classified is no longer sensitive and no longer requires special security or privacy protection it should be declassified.
- e. The originator of the classification is wholly responsible for reclassification and declassification.
- f. Overclassification should be considered to be as dysfunctional as underclassification.

It shall be the responsibility of the ICJISB to assure that appropriate classification systems are implemented, maintained and complied with by criminal justice agencies, within a given State.

#### Standard 8.6 - SYSTEM SECURITY

System security provisions should be instituted for an information system that are appropriate to the use of the system by the agency it serves, and to the sensitivity of the data in the system.

1. Protection from Accidental Loss. Information system operators should institute procedures for protection of information from environmental hazards including fire, flood, and power failure. Appropriate elements should include:
  - a. Adequate fire detection and quenching systems;
  - b. Watertight facilities;
  - c. Protection against water and smoke damage;
  - d. Liaison with local fire and public safety officials;
  - e. Fire resistant materials on walls and floors;

- f. Air conditioning systems;
- g. Emergency power sources; and
- h. Backup files.

2. Intentional Damage to System. Agencies administering criminal justice information systems should adopt security procedures which limit access to information files. These procedures should include use of guards, keys, badges, passwords, access restrictions, sign-in logs, or like controls.

All facilities which house criminal justice information files should be so designed and constructed as to reduce the possibility of physical damage to the information. Appropriate steps in this regard include: physical limitations on access; security storage for information media; heavy duty, non-exposed walls; perimeter barriers; adequate lighting; detection and warning devices, and closed circuit television.

3. Unauthorized Access. Criminal justice information systems should maintain controls over access to information by requiring identification, authorization, and authentication of system users and their need and right to know. Processing restrictions, threat monitoring, privacy transformations (e. g., scrambling, encoding/decoding), and integrity management should be employed to ensure system security.

4. Personnel Security.

a. Preemployment Screening: Applicants for employment in information systems should be expected to consent to an investigation of their character, habits, previous employment, and other matters necessary to establish their good moral character, reputation, and honesty. Giving false information of a substantial nature should disqualify an applicant from employment.

Investigation should be designed to develop sufficient information to enable the appropriate officials to determine employability and fitness of persons entering critical/sensitive positions. Whenever practicable, investigations should be conducted on a preemployment basis and the resulting reports used as a personnel selection device.



b. Clearance, Annual Review, Security Manual, and In-Service Training: System personnel including terminal operators in remote locations, as well as programmers, computer operators, and others working at, or near the central processor, should be assigned appropriate security clearances and should have their clearances renewed annually 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. To this end, each employee should receive not less than 10 hours of training each year concerning system security.

c. System Discipline: The management of each criminal justice information system should establish sanctions for accidental or intentional violation of system security standards. Supervisory personnel should be delegated adequate authority and responsibility to enforce the system's security standards.

Any violations of the provisions of these standards by any employee or officer of any public agency, in addition to any applicable criminal or civil penalties, shall be punished by suspension, discharge, reduction in grade, transfer, or such other administrative penalties as are deemed by the criminal justice agency to be appropriate.

Where any public agency is found by the ICJISB willfully or repeatedly to have violated the requirements of the standard (act), the Board may, where other statutory provisions permit, prohibit the dissemination of criminal history record information to that agency, for such periods, and on such conditions as the Board deems appropriate.

#### Standard 8.7 - PERSONNEL CLEARANCES

1. The ICJISB shall also have the responsibility of assuring that a personnel clearance system is implemented and complied with by criminal justice agencies within the State.

2. Personnel shall be granted clearances for access to sensitive places and things in accordance with strict right to know and need to know principles.

3. In no event may any person who does not possess a valid sensitivity clearance indicating right to know have access to any classified places or things, and in no event may any person have access to places or things of a higher sensitivity classification than the highest valid clearance held by that person.

4. The possession of a valid clearance indicating right to know does not warrant unconditional access to all places and things of the sensitivity classification for which the person holds clearance. In appropriate cases such persons may be denied access because of absence of need to know.

5. In appropriate cases, all persons in a certain category may be granted blanket right to know clearance for access to places and things classified as restricted or confidential.

6. Right to know clearances for highly sensitive places and things shall be granted on a selective and individual basis only and must be based upon the strictest of personnel investigations.

7. Clearances shall be granted by the head of the agency concerned and shall be binding only upon the criminal justice agency itself, except that right to know clearances for members of the Board and the staff of the Board shall be granted and shall be valid for all purposes where a need to know exists.

8. Clearances granted by one agency may be given full faith and credit by another agency; however, ultimate responsibility for the integrity of the persons granted right to know clearances remains at all times with the agency granting the clearance.

9. Right to know clearances are executory and may be revoked or reduced to a lower sensitivity classification at the will of the grantor. Adequate notice must be given of the reduction or revocation to all other agencies that previously relied upon such clearances.

10. It shall be the responsibility of the criminal justice agency with custody and control of classified places and things to prevent compromise of such places and things by prohibiting access to persons without clearances or with inadequate clearance status.

11. The Board shall carefully audit the granting of clearances to assure that they are valid in all respects, and that the categories of personnel clearances are consistent with right to know and need to know criteria.

12. Criminal justice agencies shall be cognizant at all times of the need periodically to review personnel clearances so as to be certain that the lowest possible clearance is accorded consistent with the individual's responsibilities.

13. To provide evidence of a person's sensitivity classification clearance, the grantor of such clearance may provide an authenticated card or certificate. Responsibility for control of the issuance, adjustment, or revocation of such documents rests with the grantor. In any event, all such documents must have an automatic expiration date requiring affirmative renewal after a reasonable period of time.

#### Standard 8.8 - 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. In no case should criminal justice research be used to the detriment of persons to whom information relates nor for any purposes other than those specified in the research proposal. Each person having access to criminal justice information should execute a binding nondisclosure agreement with penalties for violation.

3. Role of ICJSB. The Board should establish uniform criteria for protection of security and privacy in research programs. If a research or an agency is in doubt about the security or privacy aspects of particular research projects or activities the advice of the Board through its staff should be sought. The Board should maintain general oversight of all research projects using criminal justice information.

4. Duties and Responsibilities of the Holding Agency. Criminal justice agencies should retain and exercise the authority to approve in advance, monitor, and audit all research using criminal justice information. All data generated by the research program should be examined and verified. Data should not be released for any purposes if material errors or omissions have occurred which would affect security and privacy.

## Standard 9.1 - STANDARDIZED 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 shall be consistent with specifications prescribed in the NCIC operating manual, or if not covered in NCIC, the Project SEARCH Implementing State-wide Criminal Justice Statistics -- The Model and Implementation Environment Technical Report No. 4 and the National Criminal Justice Information and Statistics Service Comprehensive Data System guidelines. 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 that agency to assure that the basic requirements of this standard are met.

## Standard 9.2 - PROGRAMING LANGUAGE

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 ICJISB should provide the direction concerning programing language requirements already in force, or establish the requirements based on current or projected hardware installation and programing needs (especially from a system standpoint) of present and potential users. The programing language(s) shall not be system- or manufacturer-dependent.

## Standard 9.3 - 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.

## Standard 10.1 - LEGISLATIVE ACTIONS

To provide a solid basis for the development of systems supporting criminal justice, at least three legislative actions are needed:

1. Statutory authority should be established for planning, developing, and operating State level information and statistical systems.
2. Illinois should establish, by statute, mandatory reporting of data necessary to operate the authorized systems.
3. Statutes should be enacted to establish security and confidentiality controls on all systems.

## Standard 10.2 - THE ESTABLISHMENT OF CRIMINAL JUSTICE USER GROUPS

All criminal justice information systems, regardless of the level at which they operate, must establish user groups. These groups should, depending on the particular system, have considerable influence over the operation of the system, its continuing development, and modifications to it.

1. A user group should be established from representatives of all agencies who receive service from the criminal justice information system.
2. The user group should be considered as an advisory board to ICJISB and local and/or regional CJIS operating agencies assisting in establishing the operating policy for the criminal justice information system.
3. The user group should also be responsible for encouraging utilization of the system in all agencies and should be directly concerned with training provided by both their own staff and the central agency.
4. Membership in the user group should include the officials who are actually responsible for the various agencies within the criminal justice system.
5. Technical representation on the user group should be of an advisory nature, should assist in providing information to the user group but should not be a voting or full member of the user group.

### Standard 10.3 - SYSTEM PLANNING

Each State should establish a plan for 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.

### Standard 10.4 - CONSOLIDATION AND SURROGATE SERVICE

In those cases where it is not economically feasible to provide the information support functions described in Standard 3 at the organizational level specified, these services should be provided through consolidation of adjacent units at the organizational level specified, or by the establishment of a "surrogate" at the next higher organizational level.

1. Agency support should be provided within the agency requiring the support. When economically infeasible, such services should be provided by a consortium of nearby agencies of similar type (e. g., two nearby police departments). Alternatively, such services can be provided by the local CJIS on a "service bureau" basis.

2. Local criminal justice information system services, if economically unjustified for an individual locality, should be provided by a regional CJIS composed of adjacent localities. Alternatively, such services can be provided by the State CJIS on a service bureau basis.

3. State CJIS functions, if economically unjustified for an individual State, should be provided on a regional basis by the collective action of several States. Provision of these services by the next higher (Federal) level of CJIS is not appropriate.

4. Financial responsibility for the provision of services in cases where consolidation or surrogate provisions are carried out should remain at the organizational levels specified in this standard.

The basis for establishing the costs of such service, and the quality of performance deemed adequate for the provision of each individual service rendered should be expressed in contractual terms and agreed to by all parties to the consolidation or surrogate relationship.

5. In cases of consolidation or surrogate relationships, a strong voice in the policies and general procedures of the information system should be vested in a users group in which all users of the system are represented.

6. If at all practical, surrogate agencies should provide the same level of data that would be provided if the lower level agencies had their own systems.

#### Standard 10.5 - SYSTEMS ANALYSIS AND DESIGN

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

## Standard 11.1 - PREIMPLEMENTATION MONITORING

Especially in the case of major projects, a system of preimplementation monitoring should be used by the ILEC staff, and reported upon before any funds are released for actual implementation. 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 interagency considerations should be included, particularly with respect to consistency with other planned or operational information and statistical systems.

The following items should be considered in this monitoring standard:

1. System Analyses Documentation.
2. System Requirement Documentation.
3. System Design Documentation.
  - a. Functional specifications;
  - b. Component flow charts;
  - c. Data base design (or administration);
    1. Groupings of files;
  - e. Structure of data in files;
  - f. File maintenance;
  - g. File capacity;
  - h. Timeliness of data inputs to file;
  - 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.

## Standard 11.2 - 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 nonautomated equipment).

## Standard 11.3 - IMPACT EVALUATION

All major projects or programs supported by the ILEC should be evaluated in order to provide information for planning decisions. Impact evaluation should begin with an investigation of system outputs at the component level. Once individual components have been assessed as to their capability for supporting users, impact analyses should be conducted for larger aggregations made up first of multiple and then total components. This process permits criminal justice agencies to draw conclusions about the immediate and long-range effects of various inputs.

In general, an impact evaluation 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 statistic system; and (2) what relationships exist between specific features of the system and the benefits to the user.

Impact evaluation should adhere to the following criteria:

1. Installation of the impact plan. Operation of each component of the system should be evaluated. Quantifiable data that is needed to evaluate an investigative file/data base includes:
  - a. Number of inquiries or file searches per specified time period;
  - b. Number of investigative leads or clues provided per specified period;
  - c. Number of accurate versus erroneous suspects identified;

d. Number of arrests as a result of identification by the system;

e. Number of criminal cases cleared as a result of an arrest and/or conviction; and

f. Dollar value of property recovered.

This should be computed on a per capita basis and cost ratio with the system. Similar formal evaluation should be undertaken of such files as traffic citations, calls for service, case reporting, in-custody, want/warrant, court scheduling, criminal histories, and so forth.

2. Analysis of operational impacts over time. Each component of the system as well as the entire system should be regularly analyzed. These evaluations should include the more significant data suggested above and should be focused on how much more effectively an agency is attaining its goals and objectives. For information systems serving multiple agencies, the evaluations should focus on achieving integrated criminal justice system goals.

3. Analysis of attitudinal and behavioral impacts over time. The entire system should be assessed for a change in the attitudes and behavior of the users. This is a relatively subjective evaluation but can be quantified by appropriate, periodic user surveys.

4. Analysis of management and planning capabilities. The system should be evaluated to learn if it aids criminal justice managers and planners in achieving coordination of resources. For example, how many criminal justice managers used the system and how often? What degree of support did the system provide the manager? In retrospect, how accurate was the system in planning? Was it accurate, for example, in predicting the calls for service in a reporting district over the subsequent 12 months? Or how effectively was a court calendar scheduled?

5. Analysis of management decisions as they relate to the cost of criminal justice operations. The system should be designed to report on the ratio of its cost to the expenses of overall agency operations. Cost centers should be established and the expense of the system reported by user and organizational unit. Costs should also be determined for criminal justice programs and processes (e. g., public relations programs, probation programs, the prevention/suppression process, etc.) on regional bases (county, area, State, country) as well as on a user or agency basis.

The revenue derived from the service of warrants, cost of the system per suspect arrested, and cost of the system in reducing response time are a few of the possible criteria to be used for a police agency. Similar standards can be generated for court and corrections systems. It may prove worthwhile to allocate a portion of each user unit's budget to support the cost of the information system.

6. Analysis of technology or equipment. The cost of a hardware should be subjected to a tradeoff analysis. For example, if a rotating filing cabinet were installed, what would be the monetary savings and user advantages in terms of more rapid access to warrants or prisoner records, accuracy of filing, and ease of file maintenance? Similarly, for computer systems: What are the savings and advantages? Will the information be available and helpful to more people? Are there some other uses for the equipment which would affect the net cost of the system?

7. Analysis of program and policy change. All programmatic and policy changes within the criminal justice agency should be related to the influence that the information and statistical system may exert on them.

8. Evaluation of achievement. Criminal justice personnel, management, and citizens in need of service are best qualified to measure how effectively the system aids accomplishment of the agency's goals. By far, the most challenging requirement is to assess the "worth" of an information system as it relates to a particular set of goals. To illustrate: Does the information system reduce police response time from 4 minutes to 2 on an average per call for service? Or, does the system aid in rehabilitation by predicting effective treatment methods for individual offenders? This analysis will necessarily be more subjective than others.

ILL

608 east college st. / carbondale, illinois / area code 618 549-3306  
mailing address: post office box 3160 / carbondale, illinois / 62901

April, 1977

Greater Egypt Regional Planning  
and Development Commission  
Local Government Units  
and Criminal Justice Agencies

Standards for nonmetropolitan criminal justice are presented not as a remedy for system problems, but as a tool for clear identification of those problems to permit their subsequent solution.

These standards have been developed by members of the Regional criminal justice system community, other public officials, and citizens, and reflect the level of services they felt this Region is entitled to and should expect to receive.

The acceptance of these standards by local units of government and Regional criminal justice system components is the first step towards uniformity of services.

Sincerely,

Franklyn H. Moreno, AIP  
Executive Director

## ACKNOWLEDGEMENTS

The Greater Egypt Regional Planning and Development Commission wishes to acknowledge the Law Enforcement Assistance Administration for financial assistance in the preparation of these standards.

The Regional Commission would also like to acknowledge the following state and local agencies for financial assistance in the preparation of these standards:

Southern Illinois University  
Chairman and County Board of Alexander County  
Chairman and County Board of Franklin County  
Chairman and County Board of Gallatin County  
Chairman and County Board of Hamilton County  
Chairman and County Board of Hardin County  
Chairman and County Board of Jackson County  
Chairman and County Board of Jefferson County  
Chairman and County Board of Johnson County  
Chairman and County Board of Massac County  
Chairman and County Board of Perry County  
Chairman and County Board of Pope County  
Chairman and County Board of Pulaski County  
Chairman and County Board of Saline County  
Chairman and County Board of Union County  
Chairman and County Board of Williamson County  
City of Benton  
City of Carbondale  
City of Mt. Vernon  
City of Murphysboro  
City of West Frankfort  
Assembly of Local Governments Members

In addition, the Regional Commission would like to thank the many public officials, organizations, and citizens who contributed their time and energy in the development of these standards.

?

CONFERENCE COMMITTEE MEMBERS

<u>Member</u>	<u>Task Force Represented</u>
John W. Allen	Juvenile Justice
Richard D. Carter	Corrections
Elridge Cavitt	Public/Private Agencies
Sam Hiller	Courts
Donald E. Hood	Corrections
Ray Nowacki	Courts
Edward Quinlan	Police
Vernon Rich	Local Government Finance
James Rossiter	Diversion
Jesse L. Senderson	Diversion
Chester Starkey	Citizen Involvement
Galen Thomas	Juvenile Justice
Dick Vandeboom	Citizen Involvement
John R. Venskus	Public/Private Agencies
Frederick Winkler	Local Government Finance
Michael Wiseman	Police

POLICE TASK FORCE MEMBERS

	<u>Name</u>	<u>Representing</u>	<u>County</u>
1	Tobias Berger	Murphysboro Police Dept.	Jackson
	Joseph Dakin	Southern Illinois University	Jackson
3	Fred Dedman	Mt. Vernon Police Dept.	Jefferson
	Robin Dillon	Anna Police Dept.	Union
5	Roger Draves	Illinois State Police	Perry
	W. Charles Grace	Jackson County Public Defender	Jackson
7	Robert Harris	SIU Security	Jackson
	Larry Hill	Carbondale Police Dept.	Jackson
9	Robert Irvin	John A. Logan College	Williamson
	Robert Kekow	Sheriff's Department	Pulaski
11	George Kennedy	Carbondale Police Dept.	Jackson
	Charles Millikan	Sheriff	Hardin
13	Tim M. Moss	Carbondale Police Dept.	Jackson
	John V. Nelson	Sheriff	Massac
15	W. L. "Lou" Ozburn	Citizen	Perry
	Richard Pariser	Southern Illinois Enforcement Group	Jackson
17	Edward Quinlan, Vice-Chairman	Harrisburg Police Dept.	Saline
	Dennis Ralls	Cobden Police Dept.	Union
19	Max Ray	Citizen	Johnson
	William Rypkema	Carbondale Police Dept.	Jackson
21	Garold Shields	County Board	Jefferson
	Virgil Trummer	SIU Security	Jackson
23	Donald Turner	Sheriff	Alexander
	Bill Vollmer	Synergy	Jackson
25	Daryl Ward	Mounds Police Dept.	Pulaski
	C. W. Barney West	Ill. Dept. of Law Enforcement	Williamson
27	Michael Wiseman, Chairman	Williamson County Detective Unit	Williamson



COURT TASK FORCE MEMBERS

<u>Name</u>	<u>Representing</u>	<u>County</u>
1 William B. Ballard, Jr.	States Attorney	Union
2 Terry B. Brelje	Director, Chester Mental Health	Jackson
3 Arthur Casebeer	SIU, Higher Education	Jackson
4 John H. Clayton, Chairman	Chief Judge First Judicial Circuit	Williamson
5 Robert T. Coleman	Assistant States Attorney	Williamson
6 Joseph V. Collina	Public Defender for Alexander, Johnson, Massac, Pope and Union Counties	Alexander
7 Ronald Eckiss	Assistant States Attorney	Williamson
8 Bob Farrell	Prison Legal Aid Project	Jackson
9 Sam Hiller	Illinois State Police	Perry
10 Howard Hood	States Attorney	Jackson
11 Robert Howerton, Vice-Chairman	States Attorney	Williamson
12 Donald Irvin	States Attorney and Private Lawyer	Jefferson
13 Orval Leukering	Citizen	Williamson
14 Tom MacNamara	Carbondale Police Dept.	Jackson
15 Kia Malott	States Attorneys Task Force, Project Hand for 1st Circuit	Johnson
16 William Meehan	Director, States Attorneys Task Force for 1st Circuit	Johnson
17 T. D. Murphy	Carbondale Police Dept.	Jackson
18 Ray Nowacki	Citizen	Jackson
19 Dorothy Spomer	Judge, First Circuit	Alexander
20 Paul Staffey	Carbondale Police Dept.	Jackson
21 Stephen Wasby	SIU, Political Science	Jackson
22 Herman Watters	Circuit Clerk	Gallatin

GREATER EGYPT REGIONAL PLANNING AND DEVELOPMENT COMMISSION

Commission Members

Franklin County

R.A. Bonifield  
Charles Dawson  
Russell Davis  
George Tomlinson

Jackson County

Bill Kelley  
Osbin Ervin  
Reginald Stearns  
Phil Baewer

Jefferson County

Charles Covington  
Paul Dickerson  
David Sargent  
Carl Baker

Perry County

Dr. Allen Y. Baker  
J. Paul McNutt  
Gene Schumaier  
Ronald Shirk

Williamson County

William Humphreys  
Jo M. Walker  
Curtis Palmer  
Jack Murray

Assembly of Local Governments

William Schettler

Conservancy District

Frank Feltmeier

Municipal Representatives

Robert Tedrow, Benton  
Neal Eckert, Carbondale  
Rolland Lewis, Mt. Vernon  
Michael Bowers, Murphysboro  
Jack Woolard, West Frankfort

Executive Committee

Chairman -	Jo M. Walker
1st Vice Chairman -	Reginald Stearns
2nd Vice Chairman -	Neal Eckert
3rd Vice Chairman -	J. Paul McNutt
Secretary -	George Tomlinson
Treasurer -	William Humphreys
Immediate Past Chairman -	C.J. Covington

## Commission Staff

Franklyn H. Moreno, AIP - Executive Director  
A.S. Kirkikis - Director of Water Resources  
James R. Rush - Director of Criminal Justice Programs  
William Butler - Director of Economic Development  
\*Howard Skolnik - Director of Criminal Justice Standards/  
Victimization Project  
Christine Svec - Coordinator of Regional Program  
Wayne Martin - Criminal Justice Training Coordinator  
Jim W. Brown - Engineer  
Bill Boyd, P.E. - Engineer (Part-time)  
William Reichert - Planner III  
Ronald Clark - Planner II  
Robert Child - Planner II  
Saeed Khan - Planner I  
Sandra Hood - Planner I  
R. Jon Herbert - Planner I  
\*Muriel Canfield - Planner I  
Richard Newcombe - Planner I  
Michael Kain - Planner I  
David Ryan - Planner I  
Rue Gene Starr, Sr. - Manpower Specialist  
Rex Rakow - Training Specialist  
S. Eric Welles - Training Specialist  
\*James Kaitschuck - Citizen Resource Specialist  
Michael Harris - Municipal Circuit Rider  
Michael Woodring - Evaluation Sepcialist  
Joyce Jolliff - Research Analyst II  
Wendell Keene - Research Analyst I  
Peter Leibig - Research Analyst I  
Joseph Wesselman - Research Analyst I  
Barbara Poston - Research Analyst I  
Margie Mitchell - Administrator II  
Lynn Naumann - Bookkeeper  
Kay Chamness - Secretary III  
Marcia Connell - Secretary I  
Sue Kagy - Secretary I  
Joanne Tabela - Secretary I  
Betsy Prosser - Secretary I  
Michelle Stevens - Secretary I  
Glenn Gill - Planning Technician I  
Rebecca Baker - Planning Technician I  
Ellen White - Planning Technician I  
\*S.P.D. Silva - Intern  
Maurice McFarlin - Intern  
Foday Kamora - Intern  
\*Peter Wang - Intern  
\*Bridin Ashe - Intern  
\*Eric Emmerich - Intern  
Steven Banker - Intern  
\*David Reedy - Intern

\*Primarily responsible for this report.

CORRECTIONS TASK FORCE MEMBERS

<u>Name</u>	<u>Representing</u>	<u>County</u>
1 - John W. Allen	Illinois Department of Children & Family Services	Williamson
2 - Edward E. Bellamy, Ph.D.	A. L. Bowen Children's Center	Saline
3 - Champ K. Brahe, Ph.D.	Adult Parole Services, Illinois Department of Corrections	Jackson
4 - Richard D. Carter	Director of Probation, First Judicial District of Illinois	Union
5 - Barbara Hawkins	Citizen	Jackson
- Edward J. Hogan	Acting Police Chief, Carbondale Police Department	Jackson
7 - Donald E. Hood	Vienna Correctional Center	Johnson
Johnnie R. Knapp	Carbondale Police Department	Jackson
9 - Joyce Matich, Vice-Chairperson	Citizen	Williamson
Sharon Moone-Jochums, Chairperson	Interim Director University Christian Ministries	Jackson
11 - Harold E. Nelson	Illinois State Police	Alexander
Richard F. Steinhaus	Adult Parole Services, Illinois Department of Corrections	Jackson
13 - Ronnie L. Wells	Bureau of Detention Standards and Services, Illinois	
	Department of Corrections	Williamson
Donald R. White	Sheriff	Jackson

DIVERSION TASK FORCE MEMBERS

<u>Name</u>	<u>Representing</u>	<u>County</u>
Theodore H. Bollmann	Correctional Counselor, U. S. Penitentiary	Williamson
Gerald L. Daugherty	Director, Alcohol Information Center	Williamson
Pete Gentry	Illinois Commission on Delinquency Prevention	Williamson
Mark Godley, Chairman	Coordinator, Alcohol and Mental Health Franklin and Williamson Counties	Williamson
Milton A. Maxwell	Probation Officer, Murphysboro Courts	Jackson
Leslie McCollum	Regional Supt. of Schools (Representative Juvenile Justice Task Force)	Williamson
Jerry M. Reno	Carbondale Police Dept.	Jackson
James M. Rossiter	Carbondale Police Dept.	Jackson
Jesse L. Senderson	Project Hand, Diversion Program, First Judicial Circuit	Alexander
James H. Smith, Vice-Chairman	Public Defender and Private Attorney	Gallatin
Dayton L. Thomas	Private Attorney	Gallatin

FISCAL TASK FORCE MEMBERS

<u>Name</u>	<u>Representing</u>	<u>County</u>
1 Doyle Annable	Citizen	Johnson
1 Clarence Deuel	Chief, Police Dept. of Carrier Mills	Saline
2 Dick Haney	Illinois Office of Education	Jefferson
Max Heinzman	Citizen	Franklin
3 David Morris	Local Government Affairs	Williamson
W. A. Moore	Mayor, City of Grand Chain	Pulaski
Vice-Chairman		
7 Herbert Mundell	Mayor, City of Benton	Franklin
Vernon Rich	SIU	Jackson
6 William Schettler	Mayor, City of Sesser	Franklin
Joseph R. Shirk	County Commissioner	Perry
1 Paul Sorgen	Finance Director and City Treasurer	Jackson
Jo M. Walker, Chairman	Chairman, Williamson County Board	Williamson
12 Fred Winkler	Mayor, Mound City	Pulaski

CITIZEN INVOLVEMENT TASK FORCE MEMBERS

<u>Name</u>	<u>Representing</u>	<u>County</u>
Neal Jacobson	Carbondale Police Dept.	Jackson
George Kaskie	Citizen	Franklin
Harold Mullins	Civil Defense Director	Franklin
William McDaniel	Carrier Mills Police Dept.	Saline
J. C. Penn	Citizen	Jackson
Wilbert Pick	Citizen	Jackson
Walter Robinson	Citizen	Jackson
Thomas Rogers Vice-Chairman	Ziegler Mayor	Franklin
Chester Starkey Chairman	Carrier Mills Mayor	Saline
Ronald Trentacosti	Citizen	Jackson
Dick Vandeboom	Probation Officer	Saline
Bailey Williams	Citizen	Williamson

JUVENILE JUSTICE TASK FORCE MEMBERS

<u>Name</u>	<u>Representing</u>	<u>County</u>
John Allen, Chairperson	Dept. of Children and Family Services	Williamson
John Clemons	Assistant States Attorney	Jackson
Marc Cohen	Youth Services Bureau	Jackson
Pat Cullinane	Citizen	Jackson
Al Easton	Citizen	Jefferson
Peg Falcone	Status Offenders Project	Williamson
Albert Hamlin	Carbondale Police Dept.	Jackson
Doug Hammond	Southern Illinois Children's Service Center	Williamson
Dave Johnson Mr. & Mrs.	Land of Lincoln Legal Assistance	Jackson
D. V. Kern	Citizens	Perry
Leslie McCollum	Regional Supt. of Schools	Williamson
Andre McWilliams	Police Dept.	Jefferson
Michael Maurizio	Police Dept.	Jackson
John Newman	Youth Services Bureau	Franklin
Howard Peters	Ill. Dept. of Corrections	Randolph
Korman Smith	Cairo Mental Health	Pulaski
Davis Tate	Citizen	Saline
Galen Thomas	Massac Co. Mental Health and Family Counseling	Massac
Byron York	Probation Officer	Jackson



NON-CRIMINAL JUSTICE PUBLIC AND  
PRIVATE AGENCIES TASK FORCE MEMBERS

<u>Name</u>	<u>Representing</u>	<u>County</u>
Elridge Cavitt	Ill. Dept. of Corrections	Williamson
Joseph Coughlin	Southern Illinois University	Jackson
Floyd Cunningham, Vice-Chairman	Franklin-Williamson County Mental Health	Williamson
Clarence Johnson	Carbondale Police Department	Jackson
Richard Koppitz	Boys Club	Perry
John Mulkin	Ill. Dept. of Mental Health	Williamson
John Venskus, Chairman	Perry County H.E.L.P.	Perry
Bill Witherspoon	Citizen	Jackson
Peggy Walker	SIU, Dept. of Social Welfare	Jackson

**END**