



NCJRS

AUG 1 1977

ACQUISITIONS

CLEVELAND IMPACT CITIES PROGRAM
SECURITY AND PRIVACY PLAN
FOR PROGRAM EVALUATION

December 1973

**OFFICE OF THE MAYOR
IMPACT CITIES
ANTI-CRIME PROGRAM**

RALPH J. PERK
MAYOR

RICHARD L. BOYLAN
DIRECTOR

42567

NCJRS

SECTION I

SEP 2 1978
INTRODUCTION

1.1 PURPOSE OF THIS PLAN

The purpose of this plan is to analyze federal and state statutes, which have been legislated to insure the confidentiality of criminal justice information; to analyze federal guidelines and standards, which have been prescribed to insure security and privacy of computerized criminal justice information systems; and to present a plan to insure the security and privacy of the Cleveland IMPACT Cities Program Planning and Evaluation System. This plan has been prepared in strict accordance with both federal and state statutes. However, it has also been prepared in order to implement federal security and privacy guidelines and standards applicable to computerized criminal justice information systems. These guidelines and standards are far more restrictive than either federal or Ohio legislation and are the result of intensive work by two federally sponsored efforts: (1) Project SEARCH* (System for Electronic Analysis and Retrieval of Criminal Histories), and (2) the National Advisory Commission on Criminal Justice Standards and Goals. The substantive provisions of the plan reflect important security and privacy considerations expressed by the Project SEARCH Committee on Security and Privacy, as set forth in Project SEARCH Technical Report No. 2, SECURITY AND PRIVACY CONSIDERATIONS IN CRIMINAL HISTORY INFORMATION SYSTEMS (1970),

* A cooperative program of the states, funded by LEAA, organized to develop and test prototype systems which may have multistate utility for the application of advanced technology to the administration of criminal justice.

and the National Advisory Commission on Criminal Justice Standards and Goals, as set forth in REPORT ON THE CRIMINAL JUSTICE SYSTEM (1973).

1.2 BACKGROUND AND GOALS OF THE CLEVELAND IMPACT CITIES PROGRAM

The Cleveland IMPACT Cities Program is a crime-specific planning and action effort, sponsored by the Law Enforcement Assistance Administration of the U.S. Department of Justice, designed to reduce the incidence of stranger-to-stranger crime and burglary in the City of Cleveland by five percent in two years and 20 percent in five years. Seven other cities,* ranging in population size from 250,000 to 1,000,000, are also participating in the LEAA High IMPACT Anti-Crime Program.

Stranger-to-stranger crimes are homicides, rapes, aggravated assaults, and robberies, as defined by the FBI's Uniform Crime Reporting Standards, where such offenses do not occur among relatives, friends, or persons well known to each other. Approximately \$160 million in discretionary action grant funds and planning and evaluation funds from the National Institute of Law Enforcement and Criminal Justice (LEAA's research and development arm) have been made available over the Fiscal Year 1972-1974 period to (1) establish a planning agency in each IMPACT city, (2) undertake an analysis of target crimes, victims, and offenders, (3) formulate a comprehensive set of quantified, time-phased objectives

* Atlanta, Baltimore, Dallas, Denver, Newark, Portland, and St. Louis.

for IMPACT crime reduction, (4) develop programs and projects responsive to identified problems and needs, and (5) monitor and evaluate the programs and projects.

The Cleveland IMPACT Cities Program encompasses 25 projects in five major Operating Program areas: Addiction Treatment; Employment; Diversion and Rehabilitation; Deterrence, Detection, and Apprehension; and Adjudication. Figure 1 depicts the hierarchical program structure and indicates most of the projects which are operational, and some of which are now approaching completion of important milestone dates. The figure also shows the various projects as they relate to the Performance Management System (PMS) structure of the ultimate goal, four sub-level goals, five Operating Programs, and 21 of the 25 projects.* The PMS structure was developed to permit reliable and accurate evaluative measurement of program/project effectiveness and efficiency with reference to the ultimate goal, the sub-level program goals, and specific project objectives. All of these measures and objectives are set forth in detail in the Cleveland IMPACT Cities Program EVALUATION COMPONENT, a technical document published in June 1973.

To date, the Cleveland IMPACT Cities Program has either expended or encumbered nearly \$14 million in LEAA discretionary funds. The size and scope of a program of this magnitude and complexity present a number

* Four projects were funded after Figure 1 was prepared for the EVALUATION COMPONENT (referenced below) and therefore are not shown.

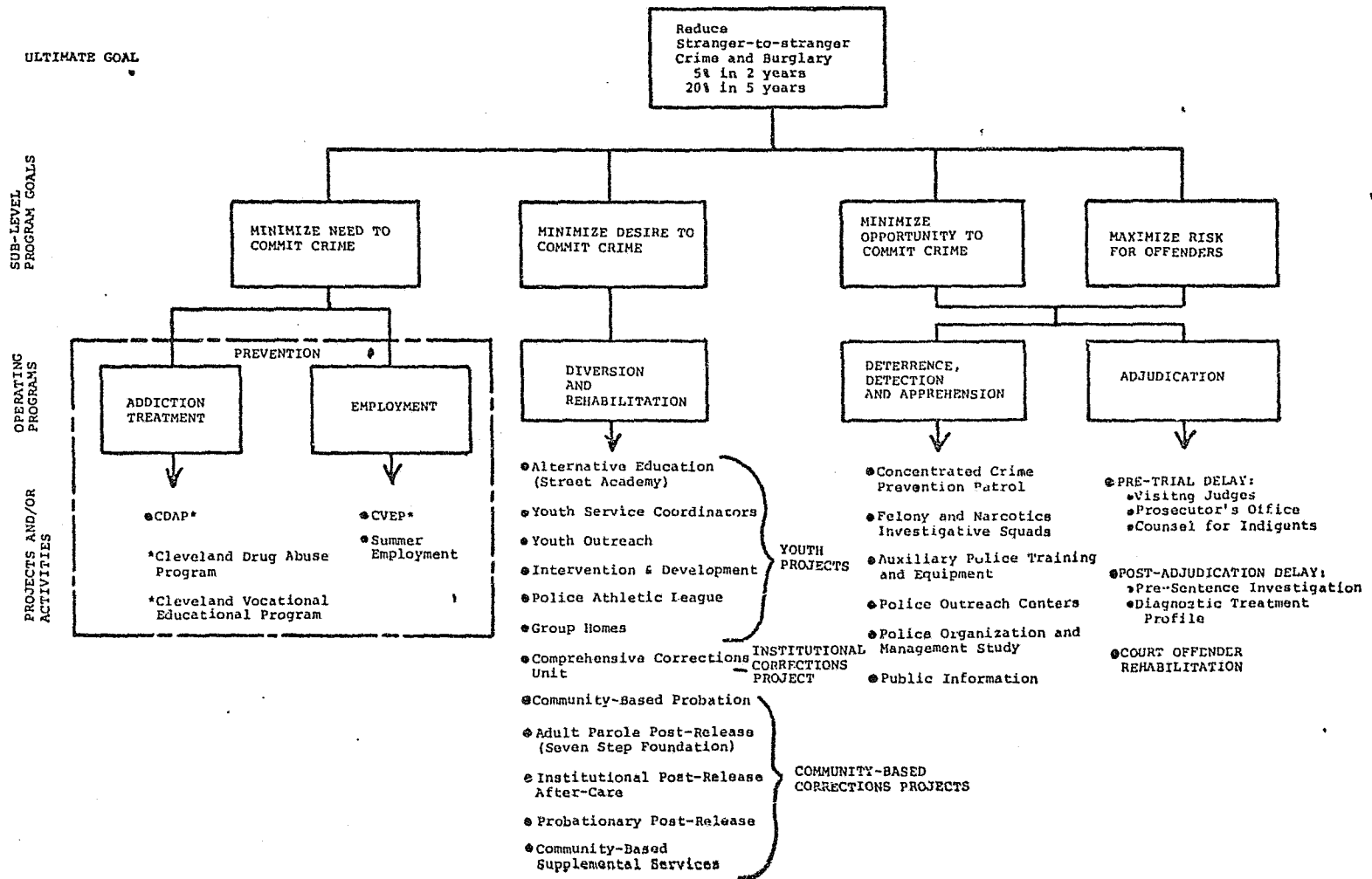


FIGURE 1

CLEVELAND IMPACT CITIES PROGRAM STRUCTURE

of special problems with regard to evaluation. A substantial number of local criminal justice agencies, both in the City of Cleveland and Cuyahoga County, are participating in the various Operating Programs and projects as well as a number of local community agencies. One of the principal challenges to rigorous evaluation is reliable collection and analysis of data from a wide variety of law enforcement, prosecutorial, defense, judicial, and correctional sources in the local criminal justice system, not to mention a number of private implementing agencies.

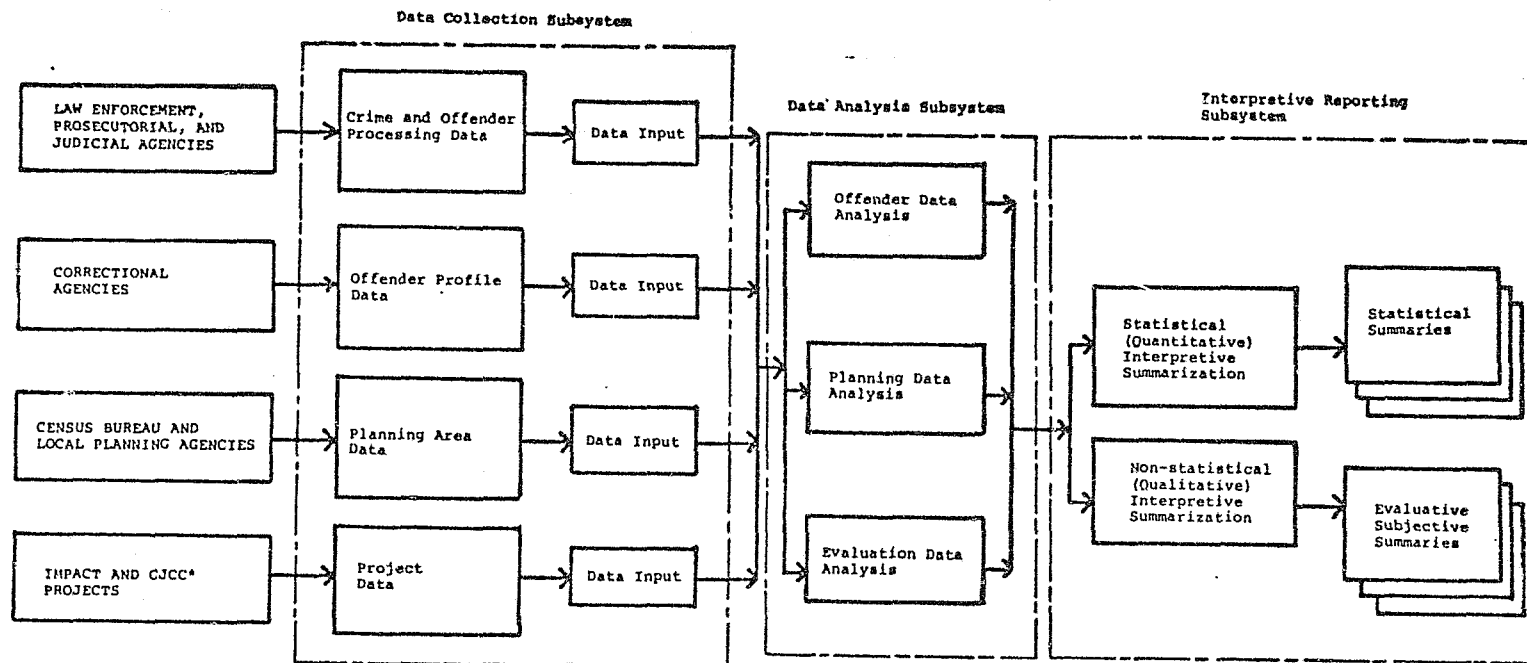
Pursuant to the EVALUATION COMPONENT, referenced above, all of the agencies currently implementing IMPACT Operating Programs and projects have been asked to collect data concerning the target populations they are serving, the types of services they are delivering, the quality of the services, the resources associated with delivery, and the results of the services -- in short, data permitting measurement of the effectiveness and efficiency of each project. The data which are collected are then analyzed, generally by computer-assisted methods, to develop the necessary evaluative profiles and measurements. Much of the data which the IMPACT Evaluation Staff intends to analyze is being collected by each project and recorded on a series of Data Collection Instruments (DCIs) specifically designed for each project. The DCIs in many instances contain data elements which relate to information about offender or client socio-economic backgrounds, prior criminal histories, current legal status in the criminal justice system

(if applicable), and client-specific operational data (such as the treatment modality of a drug abuser or the post-release status of a probationer).

Those projects which are not using DCIs as the method of data collection are capturing data as part of a pre-existing reporting routine and they have agreed to make their data available to the IMPACT Evaluation Staff. To meet the diverse data collection and data analysis requirements of the entire program, the Evaluation Staff developed and is now implementing the Cleveland IMPACT Cities Program Planning and Evaluation System (hereinafter the Evaluation System).

1.3 CLEVELAND IMPACT CITIES PROGRAM PLANNING AND EVALUATION SYSTEM

The IMPACT Evaluation System has been structured to serve two principal and exclusive types of users, namely, planners and evaluators on the Cleveland IMPACT Cities Program staff, the LEAA Chicago Regional Office staff, and the National Institute of Law Enforcement and Criminal Justice staff. Development of the Evaluation System has resulted in the creation of three Subsystems: (1) a Data Collection Subsystem, (2) a Data Analysis Subsystem, and (3) an Interpretive Reporting Subsystem. All three subsystems have been designed to be mutually supportive and to provide pertinent management, planning, and evaluation information to the IMPACT Director and the Planning and Evaluation staff. Figure 2 depicts the Evaluation System in terms of the three subsystems. When



*Criminal Justice
Coordinating Council of
Greater Cleveland

FIGURE 2
CLEVELAND CITIES IMPACT PROGRAM
PLANNING & EVALUATION SYSTEM

fully operational, the Evaluation System will provide input and reporting formats and information output reports and displays reflecting IMPACT criminal justice problems and needs for planning purposes and IMPACT effectiveness and efficiency measures for evaluative purposes at both the program and project levels.

The Data Collection Subsystem has been divided into four major areas or modules of data: (1) IMPACT crime and offender processing data, (2) IMPACT offender profile data, (3) planning area data, and (4) IMPACT program/project data. Accordingly, crime data, clearance data, offender processing data, dispositional data, and offender profile data are in the process of being collected from criminal justice agencies, funded by IMPACT, and some of the IMPACT programs/projects. The data have been organized into a series of files for computerized processing.

The basic approach underpinning development and implementation of the Evaluation System follows innovations in the collection and analysis of criminal justice statistics. The approach, often referred to as offender-based transaction statistics, case-following statistics, or subject-in-process statistics, focuses on the individual person and "tracks" the processing of the individual from point of entry in the criminal justice system (or an IMPACT project) to point of exit. Because the individual IMPACT offender or client is the only unit of count common to all criminal

justice agencies and processes, he is the thread that holds the statistical system together. By following the various paths that IMPACT offenders and clients can take, as the result of implementation of various IMPACT programs and projects, the functioning of the criminal justice system of Greater Cleveland can be statistically described in terms of the aggregate experiences of those IMPACT offenders/clients who pass through it. For purposes of the Evaluation System, the term transaction implies that there are at least two parties in every IMPACT event monitored and that the IMPACT offender or client is one of them.

As IMPACT crime, offender, planning, and project data are collected pursuant to the procedures of data capture in the Data Collection Subsystem (e.g., project Data Collection Instruments), an IMPACT/City Data Processing technical group will process the data according to a series of analytical and statistical routines (i.e., computer programs) for the editing, sorting, reduction, and presentation of data into formats useful to IMPACT planners and evaluators.

A series of computer programs have been (or will be) written in COBOL and FORTRAN which will read Data Collection Subsystem data punched on cards. These computer programs will organize IMPACT crime, offender, planning, and project data into predefined categories and aggregates for analysis. The analytical procedures are described in greater detail in Section III of the EVALUATION COMPONENT.

From the standpoint of insuring security and privacy of the Evaluation System, the Data Collection and Data Analysis Subsystems are the two most important subsystems where confidentiality problems arise. The next subsection presents a general definition of security and privacy.

1.4 SECURITY AND PRIVACY CONSIDERATIONS

The past decade has witnessed a large growth in both the number and size of criminal justice information systems throughout the country. The Evaluation System is no exception to this growth, although its purpose is restricted to research and evaluation. The Evaluation System, when fully operational, will be collecting, storing, analyzing, and reporting information based upon thousands of data elements about IMPACT crimes, arrests, charges, prosecutions, convictions, dispositions, sentences, correctional supervision, and related subjects. Given the scope of the Evaluation System, and particularly its computerized characteristics, special problems may arise concerning confidentiality. Data may enter the system which under no circumstances should ever be disseminated beyond the small group on the IMPACT Cities Program staff responsible for planning, evaluation, and monitoring. A lapse in the security and privacy policies and procedures of the Evaluation System might cause serious damage to private citizens or the criminal justice agencies and projects supported by IMPACT funding.

For example; the security of the Evaluation System might be seriously compromised (1) if unauthorized persons can add to, change, or delete entries pursuant to the processes of the Data Collection or Data Analysis Subsystems, (2) if authorized persons can make excerpts of information within the two subsystems for private motives or personal gain, or (3) if the contents of the Evaluation System or some portion of the contents can be made known to unauthorized persons or the public at large. In this context, security "refers to the protection of the system itself against intended or accidental injury or intrusion." *

Like security, the protection of individual privacy is a critical consideration in the development and implementation of the Evaluation System. Insuring privacy can result in part from making certain that the data in the system are valid, that is to say, no data entries save those which are justified and accurate in every detail. But the principal protection derives from complete assurance that the data in the Evaluation System will not be distributed to anyone outside the IMPACT Cities Program staff and that the reports produced will in no way reflect data and information about either individual IMPACT offenders or project clients. In this context, privacy refers to the protection of the interests of the people whose names appear for whatever reason in the contents of the Evaluation System.

* National Advisory Commission on Criminal Justice Standards and Goals, REPORT ON THE CRIMINAL JUSTICE SYSTEM, p. 114, Washington: GPO (1973).

The remainder of this document is organized into two sections, the first of which presents statutory materials and federal guidelines and standards applicable to the security and privacy of the Evaluation System, and the second of which outlines a plan to insure the security and privacy of the Evaluation System.

SECTION II

SECURITY AND PRIVACY REQUIREMENTS ANALYSIS

2.1 OVERVIEW

The history of state and federal action to insure security and privacy of criminal history information is recent and incomplete. The Ohio Legislature, for example, has not passed any legislation which resolves security and privacy problems and issues associated with computerized criminal justice information systems, although there are a few statutes which are concerned directly with the confidentiality of various kinds of adult and juvenile records. Similarly, neither Congress nor the Executive Branch have promulgated a comprehensive set of regulations in the security and privacy field, although some legislation has been passed, other legislative proposals have been pending in both the 92d and 93d Congresses, and LEAA has sponsored legal and technical research which has defined the major issues of security and privacy.

Each of the foregoing areas of state and federal action has been analyzed separately in order to identify (1) existing security and privacy requirements under Ohio law, (2) existing security and privacy requirements under federal law, and (3) federal guidelines and standards which the Evaluation System Security and Privacy Plan should incorporate in either full or adapted form for purposes of policy-making and/or procedural implementation.

2.2 EXISTING LEGISLATION

The new 1974 Ohio Criminal Code, which will take effect on January 1, 1974, provides in several chapters for the confidentiality of certain types of criminal justice information recorded on specific types of records.

Specifically, Chapter 2151 of the Ohio Revised Code (ORC) sets forth the jurisdiction of the Juvenile Court; Chapters 2901-2935 of the ORC set forth the new and revised classifications of criminal liability in Ohio; and Chapter 3719 of the ORC regulates possession, usage, and sale of barbiturates and narcotic drugs. Within these chapters are of course hundreds of statutes. Among them, there are only three substantive code sections * and two procedural rules which regulate record-keeping about adult and juvenile offenders and restrict the distribution of information about adults and juveniles.

In the case of juveniles, ORC Section 2151.14 provides that "the reports and records of the [Juvenile Probation] Department shall be considered confidential information and shall not be made public." These reports and records are concerned with Probation Department activities with regard to investigations, judicial actions, and supervision in juvenile cases. ORC Section 2151.18 authorizes the Juvenile Court to maintain records of all official juvenile cases brought before the Court and to prepare an annual report "showing the number and kinds of cases that

* Not including ORC Section 149.43, Availability of Public Records, which exempts from public inspection "records pertaining to physical or psychiatric examinations, adoption, probation, and parole proceedings, and records the release of which is prohibited by state or federal law."

have come before it, the disposition thereof, and such other data pertaining to the work of the Court as the juvenile judge directs or as the Department of Public Welfare directs." Such reports may be published with the approval of the board of county commissioners and distribution is restricted "to persons and agencies interested in the Court or community program for dependent, neglected, or delinquent children and juvenile traffic offenders." In addition, ORC Section 2151.358 provides for the "expungement" of juvenile records either upon application by any person "who has been adjudicated a delinquent or unruly child," or upon application by the Juvenile Court itself, "two years after the termination of any order made by the Court, or two years after [the individual's] unconditional discharge from the Ohio Youth Commission or other institution or facility to which he may have been committed." According to the terms and conditions of Section 2151.358, an individual for whom the Court finds "that the rehabilitation . . . has been attained to a satisfactory degree, the Court may order the records sealed and the proceedings in such case shall be deemed never to have occurred." The "sealing" of the records extends to the deletion of all case index references so that "the Court may properly reply that no record exists with respect to such person upon inquiry in the matter." Finally, Rule 32(C) of the Ohio Rules of Juvenile Procedure authorizes the Juvenile Court to deny or limit, under certain circumstances, inspection of the social history or report of a

physical or mental examination (about a juvenile) to counsel or "specified persons."

In the case of adults, Rule 32.2(C) of the Ohio Rules of Criminal Procedure limits, at the discretion of the judge, the disclosure of presentence reports to prosecutorial and defense counsel and requires the return of all copies of such reports to the Probation Department.

The security and privacy policies and procedures of the Evaluation System, presented in Section III below, are not in conflict with any of the strictures prescribed in ORC Sections 2151.14, 2151.18, 2151.358, Juv R 32(C), or Crim R 32.2(C), and, as will be shown in subsequent discussion, go well beyond Ohio statutory requirements.

Attention now turns to federal legislation which applies directly or indirectly to the security and privacy of the Evaluation System. In July 1970, Project SEARCH published Technical Report No. 2 entitled SECURITY AND PRIVACY CONSIDERATIONS IN CRIMINAL HISTORY INFORMATION SYSTEMS. Technical Report No. 2 recommended 23 guidelines to insure the confidentiality of criminal history information stored in computerized data banks. These guidelines served as the basis for LEAA sponsored legislation submitted to both houses of the First Session of the 92d Congress in 1971. The legislation was known as the Criminal Justice Information Systems Security and Privacy Act of 1971. The proposed Act was not

passed into law by either the House of Representatives or the Senate although the Judiciary Committees of both houses held hearings on the Act. Since 1971, Congress has passed no legislation dealing with security and privacy in a comprehensive way. However, the Crime Control Act of 1973, amending Title I of the Omnibus Crime Control and Safe Streets Act of 1968, does provide in Section 524(b) for some safeguards with respect to individual privacy. The specific language of the section is as follows:

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

Again, as with the Ohio statutes, the security and privacy policies and procedures of the Evaluation System, presented in Section III below, are not in conflict with any of the provisions of Section 524(b), and, as will be demonstrated in subsequent discussion, go well beyond the strictures of the Crime Control Act of 1973.

* For the interim citation, refer to H.R. 8152, Conference Report, p. 22, 93d Cong., 1st Sess., Report No. 93-401, Committee Print (July 26, 1973).

The legislative history of federal security and privacy legislation between 1970 and the present does include one important enactment which is directly applicable to the Cleveland IMPACT Cities Program insofar as IMPACT is funding the Cleveland Drug Abuse Program (CDAP). On March 21, 1972, Congress passed the Drug Abuse Office and Treatment Act of 1972. Section 408 of the Act is very express about insuring the confidentiality of patient records in drug abuse programs such as CDAP. Section 408(a) provides as follows:

Records of the identity, diagnosis, prognosis, or treatment of any patient which are maintained in connection with the performance of any drug abuse prevention function authorized or assisted under any provision of this Act or any Act amended by this Act shall be confidential and may be disclosed only for the purposes and under the circumstances expressly authorized under subsection (b) of this section.

Subsection (b)(2)(B) of Section 408 of the Act goes on to permit the following exception:

If the patient, with respect to whom any given record referred to in subsection (a) of this section is maintained, does not give his written consent, the content of such record may be disclosed as follows: To qualified personnel for the purpose of conducting scientific research, management or financial audits, or program evaluation, but such personnel may not identify, directly or indirectly, any individual patient in any report of such research, audit, or evaluation, or otherwise disclose patient identities in any manner. *

(Underlining supplied)

In other words, the Drug Abuse Office and Treatment Act of 1972 is highly restrictive about the disclosure of patient or client records of any individual participating in the CDAP Operating Program. Indeed, other

* 21 U.S.C. 1175.

provisions of the Act impose criminal penalties for failure to adhere to the restrictions. However, the Act does permit disclosure without individual consent for purposes of program evaluation among other carefully defined circumstances. Legal interpretation of the Act has isolated two important restrictions which have governed CDAP operations from the outset: (1) that "disclosure must be made to 'qualified personnel,'" and (2) that "such personnel must show that they plan to use the information to perform some aspect of scientific research, management or financial audits, or program evaluation." *

The security and privacy procedures of the Evaluation System, presented in Section III below, are not in conflict with any of the provisions of Section 408 of the Drug Abuse Office and Treatment Act of 1972, and indeed reinforce them. Appendix A identifies all qualified personnel in the Cleveland IMPACT Cities Program Office who will be involved in the CDAP evaluation, a copy of the Data Collection Instrument which was developed for CDAP evaluation, a description of the technical approach to be used for data analysis to support the program evaluation, and the interpretive memorandum cited above. Policy or procedural matters which are common not only to the CDAP evaluation, but also to the other Operating Program and project evaluations are discussed in Section III below.

* See SAODAP Memorandum re "Disclosure of Records by Cleveland Drug Abuse Program," Executive Office of the President, Special Action Office for Drug Abuse Prevention (September 25, 1973); see Appendix.

It should be clear from this review of state and federal legislation that while some statutes are very express in restricting disclosure of any information which might be detrimental to individual privacy, there are no requirements, guidelines, and standards which have been set forth in one comprehensive statute. For this reason, the IMPACT Planning and Evaluation staff elected to promulgate a series of policies and procedures of its own to insure security and privacy where existing legislation did not address all of the important problems and issues. As noted in the Introduction, the staff, in undertaking this task, drew upon two important sources: (1) Project SEARCH Technical Report No. 2, SECURITY AND PRIVACY CONSIDERATIONS IN CRIMINAL HISTORY INFORMATION SYSTEMS, and (2) the National Advisory Commission's REPORT ON THE CRIMINAL JUSTICE SYSTEM. Each of these documents, particularly the Commission's Report, offered valuable guidelines and standards for insuring the security and privacy of the Evaluation System. These source materials are briefly reviewed in the next section, Federal Recommendations.

2.3 FEDERAL RECOMMENDATIONS

Project SEARCH Technical Report No. 2 was published to serve as a reference document on the full range of security and privacy problems and issues which are likely to arise in the development and implementation

of any computerized data base which contains criminal justice information and especially criminal histories. The most applicable part of the report is the 23 policy guidelines which the Project SEARCH Committee on Security and Privacy recommended for either formal legislative enactment or executive policy implementation. The guidelines were drafted in the form of recommendations and were divided into five major policy areas:

1. Data Content, i. e., the types of data that will be contained in computerized files,
2. Rules of Access and Data Use, i. e., the persons who will receive the data,
3. Data Dissemination, i. e., the purposes for which the data will be used,
4. Rights of Challenge and Redress, i. e., the relationship between the system and the people whose criminal history records comprise the data bank, and
5. Organization and Administration, i. e., the organizational and administrative aspects of the system.

The SEARCH Committee defined a series of policies under each of the five categories including a security and privacy policy governing utilization of computerized criminal justice information systems for research and program evaluation.

The National Advisory Commission's REPORT ON THE CRIMINAL JUSTICE SYSTEM devotes an entire chapter to "Privacy and Security,"* and, like the SEARCH Report, proposes a series of standards to insure

* National Advisory Commission, op. cit., Chapter 8, pp. 114-138; footnote, supra at p. 11.

security and privacy. The standards are set forth in eight major categories rather than five and, like SEARCH, include one specifically to govern research:

1. Security and Privacy Administration,
2. Scope of Files,
3. Access and Dissemination,
4. Information Review,
5. Data Sensitivity Classification,
6. System Security,
7. Personnel Clearances, and
8. Information for Research.

Both the SEARCH and National Advisory Commission efforts lay the foundations for any state wishing to enact comprehensive security and privacy legislation. Indeed, the SEARCH documentation includes model statutes and administrative regulations. * Since Ohio has not yet chosen to legislate a comprehensive "security and privacy package," the IMPACT Planning and Evaluation staff has developed a series of its own policies which expand and reinforce the effect of the state and federal statutes discussed earlier and implement many of the applicable SEARCH and Advisory Commission recommendations. Since the Evaluation System

* Project SEARCH, A MODEL STATE ACT FOR CRIMINAL OFFENDER RECORD INFORMATION, Technical Memorandum No. 3, Sacramento: California Crime Technological Research Foundation (May 1971); and Project SEARCH, MODEL ADMINISTRATIVE REGULATIONS FOR CRIMINAL OFFENDER RECORD INFORMATION, Technical Report No. 4, Sacramento: California Crime Technological Research Foundation (March 1972).

is not a full criminal justice information system, but rather a data base for program planning and evaluation purposes, the staff has established six policies to insure the security and privacy of the Evaluation System, drawing upon Project SEARCH policy recommendations and National Advisory Commission standards:

1. Evaluation Design,
2. Scope of Files,
3. Access and Dissemination,
4. Data Collection Subsystem Security and Privacy,
5. Data Analysis Subsystem Security and Privacy, and
6. Interpretive Reporting Subsystem Security and Privacy.

These policies are explained in the next subsection.

2.4 IMPACT SECURITY AND PRIVACY POLICIES

The fundamental concept guiding formulation of the security and privacy policies for the Evaluation System derives from the premise that IMPACT criminal justice evaluative information, with respect to both adults and juveniles, will only include data about individuals to the extent that analysis of the data contributes to evaluative knowledge that outweighs any potential intrusion on the privacy of individuals. Privacy, as defined in the Introduction, means the protection of the interests of the individuals whose names appear for whatever reason in the contents of the Evaluation System.

The concept consequently attempts to establish a reasonable balance between an individual's right to privacy and IMPACT's and LEAA's need to collect and analyze data about individuals (involved in IMPACT programs and projects) for purposes of IMPACT planning and evaluation.

In this context, it should be added that the IMPACT Planning and Evaluation staff recognize the need to identify names and/or numbers in order to associate information across time and to conduct analyses linking activities across projects. These empirical needs, including search and link procedures, are described in detail in Sections III and IV of the EVALUATION COMPONENT. The data collection and data analysis needs will be met by qualified personnel comprising the IMPACT/Data Processing technical group. * The important point is that the IMPACT Planning and Evaluation staff will implement policies and procedures which totally preclude any identification, either by direct or indirect means, of any individual offender or client in any evaluation report and, moreover, which otherwise prohibit absolutely the disclosure of individual identities in any manner whatsoever. The six specific policies which insure the foregoing are set forth below.

2.4.1 EVALUATION DESIGN

The collection and analysis of IMPACT Operating Program and project

* The IMPACT/Data Processing technical group is composed of professional IMPACT staff, IMPACT consultants, and City Data Processing Center editors, keypunchers, information systems analysts, and programmers.

data shall include the following restrictions:

- Proposed designs of evaluation shall acknowledge a fundamental commitment to respect individual privacy interests.
- The IMPACT Planning and Evaluation staff shall fully investigate and document each proposed evaluation design.
- Identification of individual offenders and/or clients (including both adults and juveniles) shall be divorced as fully as possible from the evaluative data and, under no circumstances, shall any names, numbers, or identifier codes be disclosed to any party not authorized as a working member of the IMPACT/Data Processing technical group.
- Names, numbers, or identifier codes shall be accorded special security and privacy protection.

2.4.2 SCOPE OF FILES

Data included in the Evaluation System should be limited to those data necessary to evaluate IMPACT Operating Programs and projects in accordance with the definition of performance measures and data element listings set forth in the EVALUATION COMPONENT. A data element shall be collected, stored, and analyzed, either by manual or computerized means, only if the potential benefits from its analytical use outweigh the potential injury to privacy of individuals.

2.4.3 ACCESS AND DISSEMINATION

No data included in the files of the Evaluation System, whose content refers to names, numbers, or identifier codes of IMPACT offenders or clients shall be released to any party outside the IMPACT Planning and Evaluation staff. The

members of the technical group from the City Data Processing Center will only have access to Evaluation System data to the extent that they are involved in keypunching, programming, and data processing activities which require direct contact with the data, and then, only under circumstances of control and registration of access to Data Collection Instruments, data decks, magnetic tapes, disk files, or other storage and retrieval media. Data received and stored in the Evaluation System shall be marked and readily identifiable as IMPACT data. No remote terminal access to Evaluation System data (either to a computer's central processing unit or peripheral storage or processing device) will be permitted except by authorized IMPACT/Data Processing technical group members who have been cleared to utilize a remote terminal and are further authorized to have access to restriction control and job control language codes.

Finally, no member of either the IMPACT Planning and Evaluation staff or the IMPACT/Data Processing technical group will be permitted access to any non-IMPACT law enforcement or criminal justice data stored in computer-processed files, maintained in the Data Processing Center in a real-time, on-line, or batch mode, except where such non-IMPACT data are necessary to complete analyses between IMPACT data segments and non-IMPACT data segments (e.g., data segments concerning the arrest rates of IMPACT vs. non-IMPACT police officers).

2.4.4 DATA COLLECTION SUBSYSTEM SECURITY AND PRIVACY

The Data Collection Subsystem of the Evaluation System shall include the following restrictions:

- All completed Operating Program and project Data Collection Instruments (DCIs) and other IMPACT evaluative data shall be stored in the Cleveland IMPACT Cities Program Office in files and cabinets which are secure with the exception of data and documentation which are stored in some other medium in the Data Processing Center (for policy details concerning the latter, see paragraph 2.4.5).
- The IMPACT Planning and Evaluation staff shall establish a procedure for (1) the control and registration of locked files and cabinets containing IMPACT DCIs and evaluative data, and (2) the control and registration of all IMPACT evaluative documents (for purposes of either internal or external distribution), whose content refers to names, numbers, or identifier codes of IMPACT offenders and clients.
- The IMPACT Planning and Evaluation staff shall not release, under any circumstances, any IMPACT DCIs or evaluative data, whose content refers to names, numbers, or identifier codes of IMPACT offenders and clients, to authorized members of the IMPACT/Data Processing technical group without prior and full compliance with all requirements of the document control procedure governing release of IMPACT evaluative data and documentation.
- The IMPACT Planning and Evaluation staff shall include in the document control procedure specific requirements for the identification of all DCIs by project sequence number, the identification of any member of the IMPACT Planning and Evaluation staff or the IMPACT/Data Processing technical group to whom DCIs have been released for analytical purposes, the time of release and return of the DCIs, and the systematic logging of all of the foregoing.

2.4.5 DATA ANALYSIS SUBSYSTEM SECURITY AND PRIVACY

The Data Analysis Subsystem of the Evaluation System shall include the following restrictions:

- IMPACT DCIs or evaluative data, whose content refers to names, numbers, or identifier codes of IMPACT offenders and clients, shall only be released to the custody of authorized members of the IMPACT/Data Processing technical group (i. e., evaluators, monitors, consultants, editors, keypunchers, information systems analysts, or programmers) for temporary periods, the duration and purpose of which shall only be for performance of editorial, keypunching, programming, or data processing functions necessary to prepare analyses supporting evaluation of IMPACT Operating Programs and projects.
- IMPACT evaluative data, whose content refers to names, numbers, or identifier codes of IMPACT offenders and clients, and which are not captured on DCIs but rather stored in some other medium (e. g., cards, tape, or disk) by the Data Processing Center, as part of an already existing criminal justice reporting routine, shall be securely stored and controlled in either the IMPACT Cities Program Office or the Data Processing Center under the supervision of the IMPACT/Data Processing technical group.

2.4.6 INTERPRETIVE REPORTING SUBSYSTEM SECURITY AND PRIVACY

The Interpretive Reporting Subsystem of the Evaluation System shall include the following restrictions:

- No IMPACT interim or final evaluation report, releasable technical memorandum, or monitoring report shall include any data or documentation concerning any IMPACT Operating Program, project, or criminal justice activity which refers, either directly or indirectly, to names, numbers, or identifier codes of any IMPACT offender or client or any other individual about whom criminal justice information may be maintained.

- No CDAP interim or final evaluation report, releasable technical memorandum, or releasable monitoring report shall include any data or documentation concerning any CDAP clients which refer to client names, numbers, or identifier codes; this restriction is designed to implement the full legislative intent and public policy of Section 408 of the Drug Abuse Office and Treatment Act of 1972.
- No IMPACT DCIs or evaluative data shall be maintained on a permanent basis; all DCIs or evaluative data shall be purged of any names, numbers, or identifier codes or destroyed once all IMPACT final evaluation reports and follow-up studies have been completed.

The final section of this document outlines the plan which the IMPACT Planning and Evaluation staff has developed to implement the policies set forth above.

SECTION III

PLAN FOR INSURING SECURITY AND PRIVACY

3.1 GENERAL

The plan for insuring the security and privacy of the data contained in the Evaluation System is organized according to the six policies set forth in Section II. The six policy categories are:

1. Evaluation Design,
2. Scope of Files,
3. Access and Dissemination,
4. Data Collection Subsystem Security and Privacy,
5. Data Analysis Subsystem Security and Privacy, and
6. Interpretive Reporting Subsystem Security and Privacy.

Procedures supporting implementation of the plan are included in Appendices A and B following this section.

3.2 EVALUATION DESIGN

The IMPACT Planning and Evaluation staff shall undertake the following actions to implement Evaluation Design policies:

- The staff shall document all proposed evaluation designs for each Operating Program and/or project. The staff shall base the designs on the evaluation plans set forth in the EVALUATION COMPONENT and shall supplement existing documentation by appropriate technical memoranda. An example of such a memorandum is included in Appendix A (see the Technical Memorandum, "CDAP Data Collection, Processing, and Analysis," October 30, 1973).

- The staff shall separate, to the maximum extent feasible, all IMPACT offender and/or client names, numbers, identifier codes, and shall specify the necessary manual, software, or other safeguards to insure such separation. These safeguards will be documented by a technical or procedural memorandum.

3.3 SCOPE OF FILES

The IMPACT Planning and Evaluation staff shall only capture data which are consistent with the definitions of Operating Program and/or project performance (i. e., effectiveness and efficiency) measures, data element listings, Data Collection Instruments, and other data capture procedures set forth in the EVALUATION COMPONENT. Modifications of any of the foregoing materials will be documented by technical memoranda. The staff, in collecting any data specified either in data element listings or Data Collection Instruments, shall weigh the potential benefits for purposes of program evaluation against the potential injury to individual privacy interests, with respect to either adults or juveniles, insofar as such data elements refer to names, numbers, or identifier codes of IMPACT offenders and clients. Such judgments shall be documented in technical memoranda.

3.4 ACCESS AND DISSEMINATION

The IMPACT Planning and Evaluation staff and the IMPACT/Data Processing technical group shall not, under any circumstances, release any IMPACT data collected, stored, or processed within the Evaluation System whose

content refers to names, numbers, or identifier codes of IMPACT offenders and clients, except to authorized members of the IMPACT/Data Processing technical group.

Members of either the IMPACT Planning and Evaluation staff or the IMPACT/Data Processing technical group shall have access only to specific Evaluation System data segments and only then to the extent that they require either substantive access, on a need-to-know basis, or technical access for purposes of keypunching, programming, or data processing pursuant to a documented evaluation design.

Members of either the IMPACT Planning and Evaluation staff or members of the IMPACT/Data Processing technical group shall not be permitted access to computerized IMPACT data by remote terminal (i. e., by cathode ray tube, teletypewriter, or other terminal device) unless they are (1) authorized terminal users of the IMPACT/Data Processing technical group, should the group decide to utilize remote terminals as part of the Evaluation System hardware configuration, (2) authorized to access data pursuant to either a substantive or technical need-to-know, and (3) authorized to utilize job control language codes and software security "passwords" as described in the Software Security section of Appendix B, the IMPACT Technical Memorandum, dated December 3, 1973, entitled "Security and Privacy Plan."

Finally, no members of either the IMPACT Planning and Evaluation staff or the IMPACT/Data Processing technical group shall be authorized to know any job control language codes, software access procedures, or security codes to access any non-IMPACT law enforcement or criminal justice data stored in City Data Processing Center files, except where such non-IMPACT data (1) do not refer to the names, numbers, or identifier codes of any individual adult or juvenile, and (2) are necessary for baseline or control purposes for evaluation of specific IMPACT Operating Programs or projects in accordance with documented evaluation designs. In no case shall such access be permitted without written authorization from the custodian of the file and only then in conformity with the "access report" and other security procedures described in the Software Security section of Appendix B, referenced above.

3.5 DATA COLLECTION SUBSYSTEM SECURITY AND PRIVACY

All completed Operating Program and project Data Collection Instruments shall be stored in the Horizon Steel Storage Cabinet, Model No. 7236 with a lock (hereinafter Horizon Cabinet), located in the Planning and Evaluation Section area of the Cleveland IMPACT Cities Program Office. The Horizon Cabinet is in the sole custody of the IMPACT Planning and Evaluation staff and can be opened (by key) by only two members of the staff: the Technical Assistant (TA) for IMPACT Data Security, and the

Planning and Evaluation Secretary. The Secretary and the TA both have access to the keys to the Horizon Cabinet. The keys, during hours when the office is closed, are stored in a padlocked strong box in the Haskell Steel Filing Cabinet, Style No. 8442 (hereinafter Haskell Cabinet). The TA and the Secretary both possess keys to the Haskell Cabinet and only they know the padlock combination to the strong box. The Deputy Director of Planning and Evaluation possesses a third key to the Haskell Cabinet, but he does not know the padlock combination of the strong box in which the Horizon Cabinet keys are stored. No other members of either the IMPACT Planning and Evaluation staff or the IMPACT/Data Processing technical group possess keys or know the combinations to any of the security hardware and equipment described in this subsection.

The IMPACT Planning and Evaluation staff has established the following procedure for registration of the security of IMPACT data stored in the Horizon and Haskell Cabinets in the Planning and Evaluation Section area: The Register for Security of IMPACT Evaluation Data, shown in Figure 3, shall be posted on the Horizon and Haskell Cabinets for the purpose of registering when each cabinet is opened and when each cabinet is locked secure. When either cabinet is open, a red plastic sign, marked "OPEN" so indicates on the cabinet door or top drawer; see Standard Security Systems Catalog No. GB-13P. The green reverse side of the plastic sign is marked "LOCKED" and so indicates when the cabinet is locked secure.

The IMPACT Planning and Evaluation staff has established the following procedure for control of IMPACT data and documentation stored in the Horizon and Haskell Cabinets: The Control Log for Internal and External Handling of IMPACT Evaluation Data, shown in Figure 4, shall be posted inside the Horizon and Haskell Cabinets for the purpose of logging the following information: who has taken physical possession of any IMPACT DCI or other evaluative data, stored in either the Horizon or Haskell Cabinets; when possession was taken; the DCI project sequence or document control numbers; the purpose for which possession was taken, in conformity with the Evaluation Design policy set forth in subsection 3.2 above; and when the materials were returned.

3.6 DATA ANALYSIS SUBSYSTEM SECURITY AND PRIVACY

The security measures, software security measures, and privacy guarantees of the Data Analysis Subsystem, which the IMPACT/Data Processing technical group shall undertake to implement the Data Analysis Subsystem Security and Privacy Policy, set forth in paragraph 2.4.5 of subsection 2.4 above, are described in detail in Appendix B.

3.7 INTERPRETIVE REPORTING SUBSYSTEM SECURITY AND PRIVACY

The IMPACT Planning and Evaluation staff shall prepare no interim evaluation report, final evaluation report, releasable technical memorandum,

or monitoring report which includes any data or documentation, concerning any IMPACT Operating Program, project, or criminal justice activity, whose content refers to names, numbers, or identifier codes of any IMPACT offender or client or any other individual about whom criminal justice information of any kind is maintained.

The IMPACT Planning and Evaluation staff shall prepare no interim evaluation report, final evaluation report, releasable technical memorandum, or monitoring report which includes any data or documentation concerning CDAP whose content refers to names, numbers, or identifier codes of any CDAP client. All CDAP reports and/or memoranda, prepared by the IMPACT Planning and Evaluation staff, shall be edited to insure that any internal or releasable documentation concerning CDAP fully meets the strictures and requirements of Section 408 of the Drug Abuse Office and Treatment Act of 1972 (21 U.S.C. 1175).

The IMPACT Planning and Evaluation staff shall maintain no IMPACT evaluative data on a permanent basis and, furthermore, shall insure that all IMPACT DCIs or evaluative data are purged of names, numbers, or identifier codes, or in the alternative, are destroyed once all IMPACT final evaluation reports and follow-up studies have been completed, submitted, and approved by LEAA.

APPENDIX A

CDAP DATA COLLECTION AND DATA ANALYSIS APPROACH

This appendix consists of three documents which describe and explain the approach of the Cleveland IMPACT Cities Program Office to insure the security and privacy of CDAP client information in the course of program evaluation and which demonstrate the legality of the evaluation:

(1) a technical memorandum identifying specific professional staff members and consultants participating in the CDAP evaluation from the IMPACT Office and describing the data analysis approach, (2) a copy of the Data Collection Instrument which will be utilized to capture client specific data, and (3) a copy of the SAODAP* Memorandum re "Disclosure of Records by Cleveland Drug Abuse Program," cited supra at p. 19.

* Special Action Office for Drug Abuse Prevention, Executive Office of the President.

TO: John Caldwell *

FROM: Don Gantzer *
Wayne Town *

SUBJECT: CDAP Data Collection, Processing, and Analysis

October 30, 1973

This memorandum is in response to your memorandum on the CDAP Security and Privacy Plan, October 4, 1973.

Four general items of information were requested by you and each will now be addressed.

1) CDAP DCI

A Data Collection Instrument (DCI) has been developed in cooperation with Dave Simpson and Larry Mackie of CDAP. It is included as Attachment I and consists of three main parts:

- Client Entry Form: Section I - General Description
This section is essentially the same as Section I used for all the DCIs developed previously for other projects. One major change is the breaking out of the item, Financial Status, into two parts: Education and Employment Status.
- Client Entry Form: Section II - Project Specific
This section refers to information on every new client that is more specific to the project functions and activities.
- Client Exit Form:
This section includes information on the client as to his status at time of leaving and why he left the program. In addition, it will indicate a summary of all activities offered the client during his stay in the program.

The Client Entry Form will be completed on each new client and submitted monthly to IMPACT Cities. The Client Exit Form will also be completed and submitted to IMPACT Cities on a monthly basis. The number of entry and exit forms completed each month must agree with the PSR summary for that appropriate month.

2) CDAP Analysis

Analysis of CDAP data will be essentially handled by three programs:

- A) Summary of CDAP client characteristics and activities (similar to PSR data).
- B) Client Criminal History.
- C) Client Recidivism while in CDAP.

The names of CDAP clients will not be used in any way in the analysis for program A. For programs, B and C, the names of CDAP clients will be needed by the program but none of the output will include names. The output will consist of summary statistics such as:

* Members of the IMPACT/Data Processing technical group.

- Number of CDAP clients who have prior arrests/convictions by type of crime over various time periods.
- Number of CDAP clients who have recidivated (i.e., been arrested for a particular crime) while in the CDAP program.
- Breakdown of number of CDAP clients who are also participating in other IMPACT projects.

3) Data Base

The program data files (tape) that will be used in some way for CDAP analysis are as follows:

- CDAP DCIs (without client name)
- All IMPACT Projects Client Name-Code Matrix
- Other Project DCIs
- Police Arrest File
- Common Pleas Court File

4) Procedures

The coded DCIs will be keypunched by CDAP at their facility. The DCI forms will be stored by CDAP. The punched cards will be submitted to a particular individual (name identified at later date) at the City Computer Processing facility.

A program, developed by the above mentioned individual, will transfer the CDAP card data onto two tape files:

- All IMPACT Projects Clients Name-Code Matrix (only name, and code number).
- CDAP DCI data file (all information except name).

The cards will then be returned to the CDAP office.

The above tape files and all other data or program files are stored in a secure area at the City's Data Processing Center. Only the computer operator has access to the tape files. Each tape file has a number assigned to it and only the computer programmers working on IMPACT programs will know these numbers, along with Wayne Town and Don Gantzer of the IMPACT Cities office.

Any operation on a data file requires the submission of a Job Control Language card to the computer operator specifying the tape files to be used.

In addition to the program mentioned above which will transfer CDAP data from cards to tape files, two other master programs, ICTRAC* and ICSEG,** will be using the Name-Code data file containing the names of all IMPACT clients, not just CDAP clients.

These programs will use the Name-Code file to determine the following type of summary statistics:

- Prior criminal history of project clients.
- Arrests since becoming a project client.
- Other projects for which the same person is also a client.

These output statistical summaries will include no names. The names are used in the operation of the computer programs to obtain the summary statistics.

* IMPACT Cities Tracking

** IMPACT Cities Segment

Only persons with security clearances have access to the City's Data Processing Center. Only Wayne Town, Don Gantzer, and one or two programmers (names to be submitted later) will be aware of the format and purpose of the Name-Code file. Only through authorization of Wayne Town will any programmer be allowed to develop programs that use the Name-Code file. Under no circumstances, except by written authorization from CDAP, will the client names be printed as computer output in any format.

ATTACHMENT I
DATA COLLECTION INSTRUMENT

CDAP
Client Entry Form
(Section I - General Description)

(Right justify all numbers, left justify all alphabetic characters - e.g., names)

1-1 Project Sequence T A (1-6)
 Card Number T (9)

1-2 Name:
 Last (12-21)
 First (22-28)
 Middle (29-35)
 Maiden (36-45)
 Title: (46)
 1-Mr. 4-Jr.
 2-Mrs. 5-Sr.
 3-Miss 6-Other _____

1-3 Date of Birth Month Day Year (48-53)

1-4 Sex: 1-Male 2-Female 1-5 Race: 1-White 2-Negro 3-Oriental 4-American Indian 5-Puerto Rican 6-Mexican American 7-Other _____ (55-56)

1-6 Marital Status: 1-Single 2-Married 3-Divorced 4-Separated 5-Widowed 6-Other _____ (58)

1-7 Residential Status (live with): (60-61)
 01-Alone 02-Spouse 03-Spouse and children 04-Children only 05-Siblings 06-Parent(s) 07-Other relative 08-Friend 09-Institution 10-Other _____

1-8 Employment Status: 1-Self-employed 2-Employed by others 3-Unemployed 1-Part time 2-Full time (63-64)

1-9 Educational Status - last grade level (or equivalent) completed (67-68)
 Presently in: (70-71)
 1-Not in 2-Grade School 3-High School 4-College 5-Vocational School 6-Other _____
 1-Part time 2-Full time

ATTACHMENT I (CONTD)
DATA COLLECTION INSTRUMENT

CLIENT ENTRY FORM
(Section II - Project Specific)

Client's Name _____
Last First M.I.

2-1 Project Sequence Card Number TIA (1-6)
(9)

2-2 Date of Entry (Admittance) Month Day Year (10-15)

2-3 Current Legal Status: (17)
0-None (volunteers)
1-Free on Bail/Own Recognizance/Released to Custody
2-Held for Trial
3-Probation
4-Civil Commitment in lieu of prosecution
5-Sentenced to Commitment
6-Civil Commitment
7-Convicted and in prison/jail
8-Parole
9-Other or Unknown (specify) _____

2-4 Present or most recent charge: (19)
1-IMPACT Crime 3-Misdemeanor (non-traffic)
2-Other Felony 4-Unknown

2-5 Previously admitted to CDAP: (21)
1-Yes
2-No

2-6 Client Referred by: (23-24)
00-Unknown 07-House of Corrections
01-Self, Relative, Friend 08-Jail Screening Unit
02-Municipal Court Probation 09-Adult Parole
03-Common Pleas Court Probation 10-Ohio Youth Commission
04-Juvenile Court 11-CAAA
05-Municipal Court 12-BDA
06-Common Pleas Court 13-Other (specify) _____

2-7 Drug Usage: Primary Secondary (26-29)
00-None 06-Amphetamines
01-Heroin 07-Cocaine
02-Methadone (illegal) 08-Marijuana
03-Other opiates and synthetics 09-Hallucinogens (Psychodelics)
04-Alcohol 10-Psychotropics (Librium, Valium, etc.)
05-Barbiturates and other sedatives 11-Inhalants
12-Non-prescription, over-the-counter drugs
13-Other (specify) _____

ATTACHMENT I (CONTD)
DATA COLLECTION INSTRUMENT

46.

2-8 Treatment Location:

(31)

- 1-Harper Hall (House of Corrections)
- 2-J. Glenn Smith
- 3-Jones Memorial Center
- 4-Kinsman - 93 Clinic
- 5-Central Intake
- 6-Hough/Norwood
- 7-Hospital (Temporary Referral)
- 8-Other (specify) _____

2-9 Relationship:

(33)

- 1-Inpatient
- 2-Residential
- 3-Outpatient
- 4-Non-scheduled
- 5-Prison
- 6-Other (specify) _____

2-10 Environment:

(35)

- 1-Medical Ward
- 2-Psychiatric Ward
- 3-Live in/work in
- 4-Live in/work out
- 5-Live out/work out

2-11 Initial Treatment Approach:

(37)

- 1-Detoxification
- 2-Maintenance
- 3-Other Chemotherapy
- 4-Drug Free
- 5-Poly Drug
- 6-Other (specify) _____

2-12 Medication:

(39)

- 1-Methadone
- 2-Antagonists
- 3-Tranquilizers
- 4-Other Chemotherapy

ATTACHMENT I (CONTD)
DATA COLLECTION INSTRUMENT

47.

CDAP
CLIENT EXIT FORM

Client's Name _____
Last First M.I.

3-1 Project Sequence: T A (1-6)
Card Number (9)

3-2 Date of Exit (discharge) Month Day Year (10-15)

3-3 Legal Status at Exit: (17)

- 0-None (Voluntary)
- 1-Free on Bail/Own Recognizance/Released to Custody
- 2-Held for Trial
- 3-Probation
- 4-Civil Commitment in lieu of Prosecution
- 5-Sentenced to Commitment
- 6-Civil Commitment
- 7-Convicted and in Prison/Jail
- 8-Parole
- 9-Other or Unknown (specify) _____

3-4 If client rearrested, for what crime: (19)
1-IMPACT
2-Other Felony
3-Misdemeanors (Non-traffic)
4-Unknown

3-5 Reason for Exit: (21)
1-Satisfactory Completion
2-Satisfactory Performance upon leaving
3-Dropped Out
4-Arrested
5-Other Unsatisfaction Performance
6-All other (specify) _____

EXECUTIVE OFFICE OF THE PRESIDENT
SPECIAL ACTION OFFICE FOR DRUG ABUSE PREVENTION
WASHINGTON, DC 20506

SEP 28 1973


September 25, 1973

MEMORANDUM FOR: Peter Regner ✓
Richard W. Jacobsen

FROM: John B. Olverson

THROUGH: Grasty Crews, II

SUBJECT: Disclosure of records by Cleveland
Drug Abuse Program



Your memorandum of August 20, 1973 with enclosures, requests an opinion as to whether the Cleveland Drug Abuse Program has authority to disclose to the City Impact Office drug abuse information needed to evaluate the effectiveness of local programs.

It is the opinion of this office that the Cleveland Drug Abuse Program has authority under section 408(b)(2)(B) of P. L. 92-244 and section 401.44 of the Confidentiality Regulations (37 CFR 401.44) to disclose drug abuse information to the City Impact Office for purposes of evaluation of some aspect of a drug abuse prevention program, provided the program director is assured the information will continue to be confidential and the identity of the patient not disclosed.

Section 408(b)(2)B has two restrictions:

- (1) The disclosure must be made to "qualified personnel"; and
- (2) Such personnel must show that they plan to use the information to perform some aspect of "scientific research, management or financial audits, or program evaluation."

The letter from the Administrator of the Cleveland Drug Abuse Program states that the information disclosed will be coordinated with information received from a variety of programs for purposes of evaluation and to track IMPACT offenders to determine which of them had contact with more

than one program. The disclosure for the purposes indicated, would appear to be related to program evaluation and therefore within the authority of section 408(b)(2)(B) of P.L. 92-255. The program administrator should make sure, however, that the Cleveland Impact Office understands that it would be subject to the restrictions of section 408 with respect to the information received by it, and any disclosure of the identity of a patient would be a violation involving possible criminal sanctions.

While we are of the opinion that the authority exists to make disclosure for the purposes indicated, the question of whether the information will be properly used is within the discretion of the program administrator and if he is not given reasonable assurances that such information will be so used, he can deny the request to disclose.

CITY OF CLEVELAND

INTER-OFFICE CORRESPONDENCE

To James Murray*Date* December 3, 1973*From* Wayne Town and
Bruce Plapinger **Subject* Security and Privacy Plan

This memo details the implementation of the Security and Privacy Plan outlined in the document entitled "Cleveland IMPACT Cities Program Security and Privacy Plan for Program Evaluation" (December 1973). This memo is divided into three sections: Security Measures, Software Security, and Privacy Guarantees.

Security Measures

Two types of security measures shall be implemented in the overall data-handling system.

Because the data must be transported and handled by human beings and the data stored on relatively fragile physical devices, adequate provision shall be made for the physical protection of the data storage media. These physical security measures must guard against deliberate attempts at theft and unauthorized access as well as unpredictable accidents such as fire and computer system malfunctions. Table 1 presents a summary of the physical security measures to be implemented.

Obviously, no physical security system can be totally foolproof. The procedures outlined here will provide as much security as is possible given current technological and financial constraints.

Software Security

Once the data are in the Evaluation System, means shall be provided to insure that data are not illegally accessed or changed. These measures will be implemented via the programming system and will be totally independent of human actions except for the necessity of monitoring "access reports" which will be explained later in the memorandum.

* Members of the IMPACT/Data Processing technical group.

TABLE 1
PHYSICAL SECURITY MEASURES

PROTECTION OF	METHOD USED
Data Storage Mediums	<p>Normal Usage: Data stored on disk at computer center.</p> <p>Backup Magnetic Tape #1: Stored in fireproof cabinet in computer center.</p> <p>Backup Magnetic Tape #2: Stored in locked Horizon Cabinet at IMPACT Cities Program Office.</p> <p>Access Method: Only authorized IMPACT/Data Processing technical group staff. Each access of tape must be recorded in logbook.</p>
Data Collection Instruments	<p>While Processing: Stored in IMPACT Cities Program Office.</p> <p>Access Method: (Same as for tapes).</p> <p>After Processing: Stored in vault or other semi-impenetrable location.</p> <p>Access Method: Special approval by Director of Data Processing Center or agent authorized by Director.</p>
Keypunch Cards or Magnetic Tape	<p>While Processing: Stored in locked cabinets in computer center.</p> <p>Access Method: Only authorized keypunch operators with logbook method described above.</p> <p>After Processing: Purging or destruction of cards or return to agency.</p>
Video Display Data Entry	<p>Access Method: Only authorized data entry personnel. Logbook should record normal entries as well as description of data entered.</p>

Information in the Master Data Base (as described in Technical Memoranda #1 and #2) will be stored as illustrated in Figure 1a. Those persons required to access data in the Master File will have corresponding access to the "Security File" (see Figure 1b). When an authorized user wishes to access information, he will be required to enter a 10 character password. If the password is successfully entered, the user will be assigned a new password for his next entry into the system. This password is randomly generated by the program and replaces the current password in the Security File. When a user attempts to access information, the "protection mark" entry in the Security File will be examined to determine if the user has access privileges to the particular data item he is attempting to reference. If the access is forbidden, the user will be so informed and an entry will be made in "System Use File" (see Figure 1c), indicating that an irregular attempt was made to access the file. Otherwise, the user may access the information and an audit will be made in the access information. Also contained in the Security File will be a predefined code which indicates whether the user has edit privileges vis-a-vis the data. On every occasion where data are added to the file or data in the file are modified in any manner, a record of such action and the contents of the file before and after such addition or modification will be entered in the "Audit Trail" (see Figure 1d). The purpose of the access information file is twofold: (1) to permit tracking, verification, and reconstruction of changes to any record, and (2) to allow the IMPACT/Data Processing technical group to examine what attempts were made to access the data, both authorized and, if recorded, unauthorized. If unauthorized attempts are identified, an investigation shall be initiated to determine the exact nature and extent of such an unauthorized attempt.

Privacy Guarantees

The second important aspect of the Evaluation System will be to guarantee the accuracy and privacy of individuals' records in the data base. In the privacy area, there is little that can be done by the computer. All the responsibility lies with the IMPACT Planning and Evaluation staff members who assign the access protection codes and with those whose protection codes allow them access to "sensitive" data. In addition, the deletion of the usage of names, numbers, and identifier codes in all reports shall provide a reinforcement of privacy.

In the matter of the accuracy of data in the Evaluation System, two steps have been taken to insure that such data will be correct. First,

Figure 1a. Excerpt from Uniform Data Base File

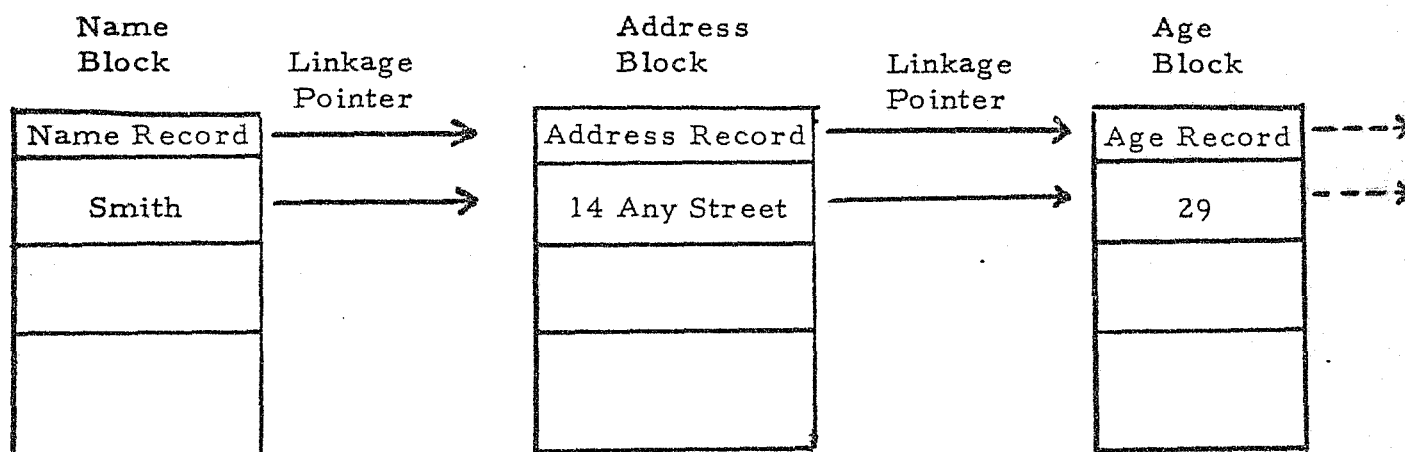


Figure 1b. Security File Format

Name	Password	Start Time (i. e., when access is allowed to begin)	End Time (i. e., when access is cut off)	Edit Word	Protection Access Māst
Example:					
Town	AXEGRCBA	0900	1700	1	11111111 etc

Figure 1c. Format of System Use File (Housekeeping)

Name	Date of Access	Time	Successful Password
Town	01/01/74	1400	Yes
Town	01/01/74	1400	Yes

Figure 1d. Audit Trail

Name	Date	Time	Old Record	New Record
Town	01/01/74	1430	oooooooooooo	oooooooooooo

all data that are prepared as inputs to the system shall be checked for proper formatting; improper formatting is the most frequent cause of record coding errors. Further, any record in which an error is detected will not be entered into the Master File and shall be returned to the contributing agency, Operating Program, or project for correction.

A final consideration for security and privacy will be the requirement that no member of either the IMPACT Planning and Evaluation staff or the IMPACT/Data Processing technical group shall discuss matters pertaining to the Evaluation System with any third party external to the IMPACT Planning and Evaluation staff or the IMPACT/Data Processing technical group.

WT/BP:df
Attachments

xc: W. Dufur
J. Caldwell

END