PRIVACY AND SECURITY PLAN

TERRITORIAL CRIME COMMISSION

March 16, 1976

TABLE OF CONTENT

Section 1

INTRODUCTION

This plan has been prepared to specifically insure that matters of privacy and security of criminal history information are accurately and explicitly addressed. In this plan, the elements of an effective, thorough privacy and security plan are presented and discussed. The requirements, problems and proposed solutions to privacy and security issues are presented in an explicit manner. The participants and action items for developing and incorporating effective privacy and security measures in existing criminal justice systems are outlined, with a schedule of dates for completion. The goals of this plan are fairly straightforward, however involved their implementation may be. They are:

* To insure the protection of interests of those people whose names appear for whatever reason in the contents of a criminal history record information system.
* To provide reasonable protection for such systems against any intentional or accidental loss, damage, or unauthorized access of information.

The plan was prepared in response to the regulations; however, its objectives and usefulness transcend that of simply complying with the regulations.

The requirement to produce a privacy and security plan is particularly timely for the territory of Guam. The Supervisory Board of the Territorial Crime Commission has requested from LEAA for FY 1977, a $120,000 grant to conduct a feasibility study of developing a computerized system for the collection and dissemination of criminal

criminal justice history. There is also underway on Guam a plan to consolidate all government computer operations. This scheme suggests a sharing arrangement of computer hardware for the purposes of collection, storage, and dissemination of data. As discussed later, the feasibility of dedicated system is cost prohibited.

It should be noted from the onset that Guam utilizes no computer hardware in the collection, storage, and dissemination of any criminal history data. All such collection, storage, and dissemination is entirely manual.

The focus of this plan will, therefore, be twofold; to provide a privacy and security plan for implementation into a manual system and to provide guidelines and suggestions for such implementation into a computer system. A product of the feasibility study will be in precisely delineating such a privacy and security plan for computer operations.

Many of the issues presented in the regulations are not addressed by existing Guam statutes. All applicable existing statutes are presented in the appropriate parts of the text. Where an issue is not covered by existing statutes and it is evident that authority, either by executive order or legislation, is required, the mechanism for obtaining the authority is presented.

It is Guam's intention to implement the total plan with respect to our manual system prior to December 31, 1977. A date cannot be projected as to when a computerized system will be implemented on Guam. It is realized that under a computer operation this will

necessitate further certifications until full compliance with the regulations is obtained.

Presently, none of Guam's criminal justice agencies have received LEAA funds specifically for the purpose of collecting, storing, or disseminating criminal history record information. However, in light of the $120,000 grant discussed supra, Guam criminal justice agencies will come under the provisions of the federal regulation.

There is no Central Repository. Such a Repository for criminal history record information will be housed at the Department of Public Safety (DPS). DPS' Records and Identification Bureau will assume the responsibility of maintaining a center for collecting, storing, and disseminating all criminal history records information. The center will be known as the Criminal Justice Information Center, (CJIC). The center will be an autonomous governmental agency directly answerable to a CJIC Committee composed of a representative from the Department of Corrections, Department of Public Safety, Attorney General's Office, the Judiciary, the Center, and two representatives from the Public at large to be appointed by the Governor and confirmed by the Legislature.

Statutory authority will be sought to establish the committee.

The CJIC Committee will be responsible for the formulation of policy, seeking legislative enactments and executive authority to implement the privacy and security plan, providing for review and appeal for challenges to criminal history records stored at the center ensuing compliance with the privacy and security plan and appointing a

manager of the Center. It is understood that the CJIC may delegate its powers via creation of complementary boards such as an appeal board. The creation of these advisory boards and their functions will be left to the discretion of the CJIC Committee.

The CJIC will be responsible for conducting the audits of user criminal justice's agencies compliance with the privacy and security plan.

Generally, each criminal justice agency will be responsible to report all dispositions occurring within its respective agency to CJIC not later than 90 days after the disposition. Ideally, such reporting would occur sooner than the ninety (90) day period. The CJIC would then file this cumulative data under the appropriate file.

Because this is a manual system, it is suggested that the attached forms be utilized for purposes of disposition reporting. Form 1 is presently in use by DPS and would be forwarded throughout the criminal justice until ultimate disposition occurred. At that point, it would be returned to CJIC. However, at each agency interval, respective dispositions would be reported to CJIC immediately. Form 1 will therefore serve as a parallel check for accuracy and completeness for agency reports. Form 2 is a status report each agency will provide in response to other criminal justice agencies' queries.

Physically, the security of the present filing system will be preserved by the following measures:

1. Security clearance of all records personnel.
2. Limited access.
3. Locked filing systems.

4. Restricted utilization of criminal history record-using right and need to know standard.

5. Segregation of all criminal records from non-criminal records.

6. Physical segregation of filing units in an area of restrictive access using rooms or spaces which can be locked and secured from unauthorized intrusion.

Security of the present system and the projected computer operation is discussed infra.

Finally, as indicated earlier, this is a plan designed to encompass Guam's present manual filing system and her projected computer operation.

Section 2

COMPLETENESS AND ACCURACY

The purpose of this section is to insure completeness and accuracy of criminal history record information. Since Guam will be recording, maintaining, and disseminating this information to both criminal justice and authorized non-criminal justice agencies, it is the responsibility of the territory to make the information that is disseminated complete and accurate to the maximum extent feasible. The completeness of this information will depend on the cooperation of each and every criminal justice agency in adhering to a set of uniform standards and procedures for submission of data to the Central Repository. These standards and the responsibilities of each submitting agency under these standards are detailed in this section of the plan. The accuracy of criminal history record information depends on strict adherence to these submission standards, the institution of systematic audit procedures, and provisions for rapid and total correction of any erroneous information when errors are discovered. The audit procedures are designed to minimize the creation or storage of erroneous information in the data bank or Central Repository. However, it is recognized that such errors are inevitable. It is further recognized that some erroneous information will be disseminated before the errors are detected. Hence, procedures for correcting any errors and for notifying all recipients of the erroneous information of the correction are provided in this section of the plan. The most practical and efficient approach to achieving com-

pleteness and accuracy in the State's criminal history data is through the development of a Central Repository.

ESTABLISHMENT OF CENTRAL REPOSITORY

Currently there is no Central Repository for criminal history information in Guam and therefore, one will be established and housed at the Department of Public Safety (DPS).

While the Central Repository will be housed at the DPS, the applicable criminal history record information applications and unit personnel will be under the management control of the Criminal Justice Information Center. This concept of management control is discussed in detail later in this section.

REPORTING OF DISPOSITIONS

Currently the reporting of dispositions is confined to individual agencies. While the dispositions are fragmented at this time, dispositions will be captured at one location. All dispositions will be reported based on positive identification. Each agency will designate one individual who will serve essentially as field staff to the Cenral Repository. It will be his function to monitor all system input for quality assurance. This qualify assurance effort encompasses the positive identification procedures.

While the detailed design of a computer design has been completed, it is planned to tie the fingerprint classification to the single tracking number of such a system. Existing statutes addressing positive identification appear below.

The subsection addressing the systematic and annual audits discusses

the procedures and inherent programmed safeguards designed to insure timely disposition reporting. In the interim, each agency records its own disposition. The existing policies for disposition reporting are as follows:

Police:

All arrestees are photographed and fingerprinted upon arrest. The arrest reports for a 24-hour period are entered on the Daily Police Bulletin by the record clerks at the police department. A Disposition Information Sheet along with the police report is then initially completed on each arrestee and forwarded to the Attorney General's office for further disposition. If the prosecutors choose not to prosecute, it is so noted on the Disposition Information Sheet. After court appearance, the prosecutor will write all dispositions on said sheet. The information sheet is then given to the prosecutor's records section for appropriate notation on its records and is then returned to the police department. The records clerks at the police department enter the disposition on the rap file, the case file, and into the (automated) manual arrest index. If the case was a felony, the disposition is returned to the police on an abstract of the prosecutor's case index. This entire process should not take more than a week. The original Disposition Information Sheet prepared by the police department is made up in duplicate and checked daily. A follow-up routine will be instigated for all delinquent dispositions.

Prosecutor:

The disposition reporting for the Attorney General's Office is fairly straightforward. Upon receipt of the police report and accompanying Disposition Information Sheet, all arrestees receive an index card numerically geared to the tracking number assigned on the Disposition Information Sheet. Dispositions received are entered on a daily basis. The Attorney General presently has a manual system. All dispositions will be noted on the assigned index card which are categorized both numerically and alphabetically. Of course such dispositional notations are recorded in the case file as well as with the Central Repository.

Courts:

The court dispositions are part of the court record. The court record coupled with the judgment papers are prepared immediately upon sentencing and are placed in the court file. This applies for both misdemeanor and felony case trials. Arraignment dispositions are also recorded on the appropriate case file.

Corrections:

The two dispositions that may occur within Corrections is that the inmate may be placed on parole or released. In either case, the appropriate form noting the disposition is simply placed in the case file and so noted on that department's index cards. The dispositions will constitute an update to the record and will be processed at least on a monthly basis.

The current disposition reporting on an individual agency basis is indeed timely; however, the dispositions do not contain complete information. The disposition reporting for the territory will create complete criminal history information. Dispositions will be reported for all agencies in the criminal justice system.

While the regulations suggest disposition reporting within 90 days, the territory's position is that all dispositions should be reported much sooner than 90 days if a system is to be dynamic enough to be of value.

The procedures that will be designed into the system to insure timely disposition reporting are discussed in the subsection addressing audits. Under a computerized system, the procedures will stem from a tracking number concept. This tracking number concept could be applied to our manual system as well. It will be necessary to conduct a disposition timing study to determine required lead times of each agency's dispositions. These lead times will constitute the expected disposition arrival times to be built into the system and will form the basis for the delinquent disposition reporting. In the interim period, the field staff at each agency will monitor the timeliness of disposition reporting. In addition to these disposition reporting procedures, there will also be a computerized procedure designed to flag all arrest records one year or older that have not received a disposition. This procedure will signify to the inquirer that further checking with the appropriate agency must be made to ascertain that the case is still pending prior to dissemination of pertinent information to all non-criminal justice agencies

not covered by the regulations. All criminal justice agencies within the territory will query the Central Repository prior to disseminating any criminal history information. The exceptions will be those cases where time is of the essence and the Central Repository is technically incapable of responding within the necessary time period to carry out the functions of the criminal justice community. This exception is most applicable to law enforcement and the prosecution attorney. This procedure will be included in the formal agreements prepared by the CRIMINAL JUSTICE INFORMATION CENTER (CJIC). Monitoring compliance for this procedure will be the responsibility of CJIC.

These disposition reporting procedures although oriented toward our manual system, are also directed to viewing a computerized criminal justice collection and dissemination system which is in the planning and design stage. These systems, as discussed earlier, will be housed at the Central Repository under the management control of CJIC.

In the interim all criminal justice agencies subject to the regulations will agree to comply to the fullest extent possible with all aspects of the regulations. Particular emphasis will be placed on the procedures listed below. Non-compliance by any agency subjects it to the sanctions discussed later in this section.

> Prior to disseminating information to a non-criminal justice agency or individual pertaining to an arrest record one year or older which has no disposition recorded, a telephone call will be made to the appropriate agency (Prosecutor, appropriate court, etc.) to determine if the case is still pending. Non-criminal justice agencies will be required to sign a notice prior to dissemination of the arrest record as discussed later in this Section under Notices. Signing of notices will also be required for any secondary dissemination.

Criminal history data dissemination will be limited to agencies and/or individuals as specified in this plan. Such agencies and/or individuals as well as the limitations on data usage are identified in the Federal regulation entitled Criminal Justice Information System, [Fed. Reg. Vol. 40, No. 98].

Limits on Dissemination

Generally, Guam has not enacted any legislation protecting the confidentially of criminal justice records. The general concept of these statutes should be that criminal justice agencies should share among themselves only that information which is relevant to their statutory responsibilities; non-criminal justice public agencies and officials should obtain data only where they have specific statutory authorization to use it. Specific Guam statutes that relate to law enforcement records appear below.

"Section 6700. Title. This Chapter shall be known as the Records Management Act. [Public Law authority after Section 7610.]

Section 6701. Definitions. Unless the context otherwise requires, the definitions set forth in this section govern the construction of this Chapter:

(a) 'Records' means document, book, paper, photograph, sound recording or other material, regardless of physical form or characteristic, made or received pursuant to law or in connection with the transaction of official business. Library and museum material made or acquired and preserved solely for reference or exhibition purposes, extra copies of documents preserved only for convenience or reference, forms, and stocks of publications are not included within the definition of records and are referred to herein as non-record materials.

(b) 'Agency' means any department, office, commission, board or other unit, however designated, of the Executive Branch of the government of Guam. [Public Law authority after Section 6710.]

Section 6702. Director. The Director of Administration; hereinafter referred to as the 'Director' shall establish and administer in the Executive Branch a record management program, which will apply efficient and economical management methods to the creation, utilization, maintenance, retention, preservation and disposal of records. [Public Law authority after Section 6710.]

Section 6703. Duties of Director. The Director shall, with due regard for the functions of the agencies concerned:

(a) Establish standards, procedures, and techniques for effective management of records;

(b) Make continuing surveys of paper work operations and recommend improvements in current records management practices including the use of space, equipment and supplies employed in creating, maintaining, storing and servicing records;

(c) Establish standards for the preparation of schedules providing for the retention of government records of continuing value and for the prompt and orderly disposal of government records no longer possessing sufficient administrative, legal or fiscal value to warrant their further keeping;

(d) Establish standards for the reproduction of records by photography or microphotographic processes with a view to the disposal to the original records.

(e) Obtain reports form agencies as are required for the administration of the program. [Public Law authority after Section 6710.]

Section 6704. Duties of agency heads. The head of each agency shall:

(a) Establish and maintain an active, continuing program for the economical and efficient management of the records of the agency;

(b) Make and maintain records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures and essential transactions of the agency designed to furnish information to protect the legal and financial rights of the government and of persons effected by the agency's activities;

(c) Submit to the Director, in accordance with the standards established by him, schedules proposing the length of time each government record warrants retention for administrative, legal or fiscal purposes after it has been received by the agency. The head of each agency also shall submit lists of government records in his custody that are not needed in the transaction of current business and that do not have sufficient administrative, legal or fiscal value to warrant their further keeping for disposal in conformity with the requirements of Section 6707;

(d) Cooperate with the Director in the conduct of surveys made by him pursuant to the provisions of this Chapter. [Public Law authority after Section 6710.]

Section 6705. Legislative and Judicial branches. Upon request, the Director shall advise in the establishment of records management programs in the legislative and Judicial branches of government. [Public Law authority after Section 6710.]

Section 6706. Records not to be damaged or destroyed. All records made or received by or under the authority of coming into the custody, control or possession of public officials of this government in the course of their public duties are the property of the government and shall not be mutilated, destroyed, transferred, removed or otherwise damaged or disposed of, in whole or in part, except as provided by law. [Public Law authority after Section 6710.]

Section 6707. Disposal of records. Records may be destroyed or disposed of in accordance with the provisions of this Chapter if it is determined by the Director, the Attorney General and the agency head concerned that such records have no further legal, administrative, fiscal, research or historical value. [Public Law authority after Section 6710.]

Section 6708. Reproduction of records on films; disposition of original.

(a) The head of any agency having the care and custody of any record may cause the same to be photographed, microphotographed or otherwise reproduced on film.

(b) When such records are photographed, microphotographed or otherwise reproduced on film, if it is determined by the Director, the Attorney General

and the agency head concerned, that the original record has no further legal, administrative, fiscal, research or historical value, the same may be disposed of in accordance with the provisions of this Chapter and thereafter the photograph, microphotograph or reproduction on film shall be deemed to be an original record for all purposes, including introduction in evidence in all courts or administrative agencies. A transcript, exemplification, facsimile or certified copy thereof shall, for all purposes recited herein, be deemed to be a transcript, exemplification, facsimile or certified copy of the original record.

(c) Where certain records are required to be kept a specified length of time or permanently, or to be destroyed by specific methods or under specific supervision, and where such records are photographed, microphotographed or reproduced on film said film may be substituted for the original records may be destroyed in the manner and under conditions prescribed in Subsection (b) above. [Public Law authority after Section 6710.]

Section 6709. Destruction of non-record materials. Non-record materials, if not otherwise prohibited by law, may be destroyed at any time by the agency in possession of such materials without the prior approval of the Director. The Director may formulate procedures and interpretations to guide in the disposition of such materials. [Public Law authority after Section 6710.]

Section 6710. Rules and regulations. The Director shall, subject to the approval of the Governor and promulgation by Executive Order, make such rules and regulations as are necessary or proper to effectuate the purposes of this Chapter. [This Chapter added by P.L. 6-64, effective February 26, 1962, renumbered to Chapter IX by P.L. 7-87, effective July 19, 1967. Section 6702 amended by P.L. 8-179, effective August 23, 1966, and by P. L. 9-239, effective August 13, 1968.]"

PENAL CODE

Section 113. Larceny, destruction, etc., of records by officers having them in custody. Every officer having the custody of any record, map, or book or of any paper or proceeding of any court, filed or deposited in any public office, or placed in his hands for any purpose, who is guilty of stealing, wilfully destroying, mutilating, defacing, altering or falsifying, removing or secreting the whole or any part of such record, map, book, paper, or proceeding, or who permits any other person so to do, is punishable by imprisonment for not less than 1 nor more than 5 years. [Enacted 1953.]

Section 114. Larceny, destruction, etc., of records by other persons. Every person not an officer such as is referred to in the preceding section, who is guilty of any of the acts specified in that section, is punishable by imprisonment not exceeding 1 year, or by fine not exceeding $100, or by both. [enacted 1953.]

Section 115. Offering false or forged instruments to be filed of record. Every person who knowingly procures or offers any false or forged instrument to be filed, registered, or recorded in any public office in the Territory of Guam, which instrument, if genuine, might be filed, or registered, or recorded under any law of the Territory of Guam or of the United States, if guilty of a felony. [Enacted 1953.]

Section 115a. Forging, stealing, mutilating, and falsifying judicial and public records and documents. Whosoever, in any matter within the jurisdiction of any department, board, commission, or agency of the government of Guam, knowingly and wilfully falsified, conceals or covers up by any trick, scheme, or device a material fact, or makes any false, fictitious or fraudulent statements or representations, or makes or uses any false writing or document knowing the same to contain any false, fictitious or fraudulent statement or entry, shall be guilty of a misdemeanor. [Added by P.L. 6-28, effective August 5, 1961 as Section 115.1; renumbered by editor]

GOVERNMENT CODE

Section 47061. Information as confidential. Neither the Director nor any other officer or employee of the Department of Commerce may--

(a) use the information furnished under the provisions of this Chapter for any purpose other than the statistical purposes for which it is supplied; or

(b) make any publication whereby the data furnished by any particular establishment or individual under this Chapter can be identified. [Added by P.L. 9-9, effective February 21, 1967.]

Section 47063. Wrongful disclosure of information. Whoever, being an officer or employee of the Department of Commerce, publishes or communicates, without the written authority of the Director, any information coming into his possession by reason of his employment under the provisions of this Chapter shall be fined not more than one thousand dollars ($1,000.00) or imprisoned not more than one (1) year, or both. [Added by P.L. 9-9, effective February 21, 1967.]

RULES OF PROCEDURES FOR THE JUVENILE COURT OF GUAM

Rule 9. Classification and Availability of Court Records

(a) PROCEDURAL RECORDS.

Procedural records shall include the docket, petitions, citations, summonses, orders, calendars, index cards, and minutes. [Effective July 31, 1969.]

(b) SOCIAL RECORDS.

Social records shall include reports of social investigations, probation treatment or supervision, psychological or psychiatric examination reports, and other reports concerning family life or compositions, school or occupational history, physical condition, foster home placement and delinquent behavior of children. [Effective July 31, 1969.]

(c) AVAILABILITY.

All procedural and social records in juvenile causes and all social records in adult cases shall be strictly safeguarded from indiscriminate public inspection. The court may, in its discretion, whenever the best interest or welfare of a child or adult or where other good cause makes such action desirable or helpful, permit inspection of any procedural or social record, except that procedural and social records shall be available on a confidential basis, without an order of the court: to the probation officer and his assistant; to social workers of the Department of Public Health and Welfare; to the Department of Corrections; to the Attorney General or his representative; to a judge of the territory of Guam; and to the Governor of Guam. Social records shall not be used as evidence during the trial or hearing of any person. [Effective July 31, 1969.]

There is no existing legislation that specifically addresses the dissemination and collection of criminal justice information. The CJIC Policy Committee that has been formed must pursue such specific legislation.

It must also be a function of the CJIC Policy Committee to explore and make recommendations as to what data elements may be disseminated. In the interim the regulations must be relied on for guidance. This

policy committee will be made aware of the regulations and their recommendations will encompass total compliance.

From the standpoint of public safety communication, only information required to protect the life and safety of the officer in the street will be released over the air.

Agreements:

Where Guam has no current legislation specifying appropriate civil or criminal sanctions for violation of the regulations, written contractual agreements between disseminating and receiving agencies will be prepared by the Attorney General's Office by December 31, 1976 to meet the objectives of the regulations.

The agreements will specify that the dissemination of criminal history record information to a receiving agency is subject to cancellation if the receiving agency violates the requirements relating to redissemination, internal use and physical security.

The agreement will also stipulate that the receiving agency may be subject to sanctions, levied by the attorney general, for violating the regulations.

Once an agreement has been signed between a disseminating agency and a receiving agency, the agreement will be binding for all future disseminations of criminal history information. These agreements may be in the form of a standard contract by the territory for use by all agencies subject to the regulations.

Any agency disseminating criminal history record information to non-criminal justice agencies covered by the regulations, and/or individuals having legislative or executive authority of access to such information for specific purposes will also make contractual agreements similar to those required for criminal justice agencies. Such agreements will also provide for disseminated information and all copies thereof to be returned to the disseminating agency or destroyed once the information is no longer needed for the purpose for which it was disseminated.

Notices:

Criminal history record information will be disseminated, where applicable, to agencies not directly subject tp the regulations. These agencies will be made aware of the provisions of the regulations with written notices prepared by the Attorney General's Office by December 31, 1976 in order to prevent unauthorized disclosure. The written notices are an essential procedure and each disseminating agency subject to the regulations will bear the burden of giving such notice to the receiving agency of the requirements of the regulations.

The notices are provided to safeguard the privacy of individuals to whom the information relates. The notices will specify restrictions on dissemination and internal agency use and will provide adequate security procedures consistent with the regulations.

The notices will include, but not be limited to the following:

* Name of agency disseminating data

* Name of agency or individual receiving data

* Specific reason for dissemination of data

* Is agency or individual cognizant of the regulations and agreeable to abide by them where applicable

* Specifications or restrictions, internal agency use and secondary dissemination

* Compliance with adequate security procedures consistent with the regulations.

Sanctions:

Sanctions prepared by the Attorney General's Office by December 31, 1976 will be provided for violations by agencies not subject to the regulations which are given criminal history information. The sanctions will subject these agencies in violation to equivalent or greater penalties than those applicable to agencies which fall under the regulations. Sanctions against these agencies in violation will be applied by the Office of the Attorney General.

Secondary Dissemination:

An agency or individual possibly having received dissemination of criminal history information will be subject to certain restrictions or secondary dissemination of such information. Secondary dissemination by any agency, whether covered by the regulations or not, will be required to provide a notice of such dissemination restrictions to the agency or individual who is in receipt of such information. The disseminating and receiving agency or individual will be subject to the same sanctions as an agency covered by the regulations.

Validation and Verification:

Before any dissemination takes place, disseminating agencies will be certain that the potential agency is an agency permitted to receive such information under the regulations. If a potential criminal justice recipient claims to be authorized to receive information pursuant to a statute, executive order, or court order or rule, the disseminating agency will review the text of such authority prior to dissemination. If the disseminating agency is not certain that the rule, statute, or order is proper authority for dissemination, it will refuse to release the information pending the opinion of the Attorney General.

Verification for individuals receiving their own criminal history record information will be made on the basis of fingerprints or identification by recognition.

Specific Guidance to Personnel:

It is recognized that all personnel who are responsible for assessing and maintaining sensitive files are in a position to either purposely or accidentally disclose confidential information. For this reason, Guam will initiate investigations of all personnel employed in this capacity to determine trustworthiness, stability and freedom from behavior that might lead to their being compromised. In addition, adequate training is provided to ascertain that sensitive data, both automated and manual, is handled properly.

A stipulation in the compliance agreements made with each agency governed by the regulations will be to familiarize all new employees,

as part of their orientation, with the regulations.

AUDITS AND QUALITY CONTROL

CJIC, via the aforementioned field staff, will be responsible for monitoring compliance with restrictions set out in the regulations. This will be addressed by requiring that appropriate records be kept of record disseminations and that a designated agency be responsible to conduct an annual audit of the Central Repository and a representative sample of criminal justice agencies to verify adherence to the regulations.

There will be two different kinds of audits, systematic audit and annual audit.

Systematic Audit:

The systematic audit process for Guam is the combination of systems and procedures employed both to guarantee completeness and to verify accuracy of records. These systems and procedures as described on the following pages will be inherent in the design of the computerized criminal justice information system which is in the design and planning stages, as well as in the present manual system. The systematic audit will deal with checking on completeness to provide a means for monitoring the submission of disposition data. These procedures are applicable to either a manual or computerized system which fall under the regulations. The systematic audit procedures will be a significant factor in the certification process where the affected agencies agree to comply with all the regulations.

CJIC will institute a delinquent disposition monitoring system for the complying agencies which will be based on estimating expected arrival dates for dispositions, which reflect anticipated processing, for each type of criminal offense. If an expected disposition is not received by the estimated due date, the inherent application software provided by the responsible agency at the Central Repository will automatically flag the record and provide information to that agency on whom to call to obtain disposition status. This information will then be reported to CJIC who will, pending investigation, withhold the dissemination of information covered under the one-year rule to agencies maintaining terminal access to the system and which are prohibited from receiving the information covered. These procedures will be covered under the section entitled Security.

Edit and Verification:

Accuracy checks during the computerized and manual edit and verification process will provide controls and inspections on the input to the system to insure integrity. In both manual and computerized systems, the audit will insure that all record entries are verified and appropriately edited prior to entry, and that source documents are properly interpreted. Audit procedures will include random inspection of the records compared with source documents to determine if data handling procedures are being correctly followed.

The field staff will be responsible for quality assurance of manual files and quality assurances for a computerized system shall be developed with the design and planning of such system.

Audit Trails

To insure that a maximum level of system accuracy is maintained, an audit trail will allow for the tracing of specific data elements back to the source document. The audit trail will encompass all participating agencies in the criminal history records system and additionally will reflect specific individuals who have made entries on source documents or input formats supporting the system. The specific audit procedures have not been developed at this time. These procedures, however, will evolve during the development of the agreements, notices, sanctions, and the implementation of this plan.

Dissemination Logs:

The audit trail covering input to the system will follow records of transactions of disseminated data over the full cycle of collection, storage, and dissemination of criminal history record information. Logging will be required for the support of the audit process and also as a means of correcting erroneous dissemination.

All agencies covered by the regulations will maintain a listing of the agencies or individuals both in and outside of the territory to which criminal history record information is released. This listing will be preserved for a period of not less than one year from the date of release. Such listings will indicate, as a minimum, the agency or individual to which information was released, the date of the release, the individual to whom the information relates, and the items of information released. The listings will include

specific numeric or other unique identifiers to provide positive identification links between information which is disseminated and the record from which the information was extracted.

Immediate notification will be provided by the disseminating agency to recipient agencies known to have received criminal history record information after inaccurate data has been entered on the record. Corrections to records will be forwarded immediately to all appropriate agencies in hard copy forms such as letter or computer printout. Agencies to which corrections were sent and the date that the notifications were released will be recorded by the disseminating agency.

Annual Audit:

Annual audits of a representative sample of criminal justice agencies chosen on a random basis will be conducted under the direction of the CJIC to verify adherence to the regulations and that appropriate records will be retained to facilitate such audits. An audit of each criminal justice agency in Guam will be conducted annually to ensure the accuracy and completeness of data maintained at the Central Repository and to insure that the other provisions of the regulations are being upheld.

The annual audits will be performed under the direction of the CJIC of criminal justice agencies for both manual and computerized systems. Dispositions, dissemination logs, and secondary dissemination logs will be audited both at the Central Repository and agencies covered by the regulations utilizing a sampling technique based on population

served. Specific records will be examined by the audit at the repository level and will be traced through internal update procedures back through field input processing to terminate at the source document. Areas to be reviewed will include, but not be limited to, review of the systematic audit procedures, an examination of the evidence of dissemination limitations, security provisions, and the individual's rights of access. Local agency audits will include annual audit of dissemination logs and secondary dissemination logs for each agency. This process will provide an annual audit of each agency in the territory. Specific cases of records events will cover a random sampling throughout all agencies. The annual audit report will be prepared and acted upon by the CJIC. The Attorney General's Office will be responsible for the levying of any sanctions for those agencies not adhering to the provisions of the regulations.

Local agencies will be responsible for providing the necessary documents and data elements to support the annual audit at the point of data entry from which criminal history information stored at the repository is derived, which should include, but not be limited to, arrest indices and reports, prosecution dispositions, court calendars or appropriate indices, correctional reports, parole reports and probation reports. Other documented information necessary to support annual audits are complete logs of dissemination maintained at each point authorized to release criminal history record data. These logs will include at a minimum the names of all persons or agencies to whom information is disseminated as well as the date of

release and any additional data elements to be contained in the dissemination logs which will appropriately complete the dissemination audit trail.

SECURITY

Information systems must be made secure against natural and human forces that could damage, destroy, or tamper with them. Guam recognizes its responsibility to control system access and maintain strict accountability for system operations. The control and accountability encompasses the Central Repository and all other data processing installation subject to the regulations.

This subsection of the plan addresses the three topics listed below:

* Management control and personnel selection
* Hardware and software security measures
* Physical security measures.

Management Control and Personnel Selection:

> To assure accountability for the operation of the system, a criminal justice agency is required to have the ability to set and enforce computer [manual] operations policy. To meet this requirement, the designated agency should be able to set priorities for user access, determine eligibility for direct access, apply sanctions for misuse of the system, select and dismiss staff, institute physical security measures and perform other administrative functions normally associated with the management of operations. 20.21 (f) (3).
>
> Each criminal justice agency presently employs its own staff for the maintenance collection and dissemination of criminal justice information. Individual agencies are responsible for their personnel selection and security clearance.
>
> The Central Repository will be housed under the Department of Public Safety but all of its employees will be employed and solely responsible to the CJIC. To ensure uniformity

among all agencies CJIC will develop the security measures affecting all agencies. CJIC will be responsible for monitoring for compliance and violation by agency employees will be handled by the agency-employer.

The proposed computer operations will as part of its plan and design implement managerial control and personnel selection procedures relevant to the criminal justice application systems.

Managerially, individual agencies will be responsible for personnel selection, security clearance, sanctioning employee misconduct. CJIC will be responsible for its own personnel selection, security clearances, sanctioning employee misconduct and also for developing general security measures. It is recognized however, that each agency is entitled to tailor general security measures into its own plan providing its measures are not more liberal than the general measures.

Guam will provide for a personnel clearance system for use in agencies which have the responsibility for maintaining or disseminating criminal history information. Guam will also establish procedures for granting clearances for access to criminal history information as well as areas where criminal history data is maintained. Clearances will be granted in accordance with strict right-to-know and need-to-know principles. The personnel clearance system will allow for selective clearances, allowing less than unconditional access to all areas. Clearances will be selected to the point of denying access because of the absence of the need-to-know. Clearances granted by one agency will be given full faith and credit by another agency. Ultimate responsibility for the integrity of the persons granted right-to-know clearances remains at all times with the agency granting the clearance. 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 will be given of the reduction or revocation to all other agencies that previously relied

upon such clearances.

Specific training requirements will be set forth for all personnel directly associated with the maintenance or dissemination of criminal history data. The training program will include the creation of a training manual as well as training sessions to brief all personnel regarding the rules and regulations.

SECURITY MEASURES (MANUAL)

The Central Repository will be housed within the Department of Public Safety. However, the management control of the Central Repository will be under the CJIC.

Guam will develop effective controls for securing present facilities and files against improper or unauthorized use. Security will be based upon four measures which help to prevent unauthorized persons from access. These measures are (1) the record and filing areas for each agency and the Central Repository will be open during specific working hours; (2) the filing cabinets and area for examination of records will be in open areas easily observable; (3) a password or similar code will be required to gain initial access; (4) users will have access to only authorized files and records.

The access rights of a user will be explicitly denoted in any situation where partial right exist, e.g., for a limited access file or where reading is permitted but changes and deletions are not. An authorization table will be provided each agency by CJIC showing a list of authorized users of the data and their access rights. Access

to this table will be strictly limited to persons authorized to modify the table and will be stored separately from the files and record.

A personal identification number or badges, will serve for authentication of a user's identity and will be used to authenticate the authorization of a user to gain access to a file.

Duplicate files will be created as a countermeasure for unauthorized destruction of original files and will be stored in a safe storage area. Duplication shall occur by means of microfilming to save in costs of replication and storage.

Data Entry:

The CJIC, with management control of the Central Repository, will have the authority to require that a specific report which fails to satisfy the standards of accuracy or completeness will be excluded or deleted from individual record information.

Where information is submitted to the user agency center on reporting forms, the responsible center will establish procedures for destroying these forms or storing them in a secure environment after the information is noted in the file or record system.

SECURITY MEASURES (HARDWARE AND SOFTWARE)

The general measures securing a manual have equal application toward a computer system.

Technical capabilities of the computer itself can protect the system from compromises: These security feature would include protection through the identification, verification, and authorization of persons, data files, and access modes within the system.

Many systems allow a user at a remote location to access the computer via telecommunication facilities and terminal devices. Therefore, an identification code of a terminal user will be implemented for each remote terminal as a precondition for entering the files. The terminal being used will also be positively identified. On a batch job not submitted at a terminal, the job card will carry the identification code. Within each agency, terminal use will be assigned to a limited and identified group of individuals.

As with a manual system, access rights of a user will be explicitly denoted and an authorization table listing authorized users of the data and their access rights will be provided and stored separately from the data.

For particularly sensitive data, a callback procedure will be instituted; in addition to the recognition of the personal identification number, to authenticate the identity of users requesting confidential data from remote terminals.

The computer will be programed to log the identity of all users, and the date of access. This information shall be maintained for 12 months.

The security software utilized in data storage will establish the proper authorizations to control inquiry and update. This authorization applies to all resources to which a user can have access, and to the mode of access.

The security programs in either the manual or computer operation will be designed wherever technically possible in such a way that neither cannot be compromised. As new techniques become apparent for bypassing the security facilities, the programs will be modified within the existing hardware constraints to seal the leak.

Data will be stored in a data base bank management classification system according to scope or permitted access and sensitivity of the data.

Confidential criminal justice records that are maintained on-line in a time shared, remote access computer system will be either password protected or have some form of inscription that at least prevents accidental disclosure, or both.

The more sensitive the data the more complex will be inscription for transmission purposes. As a minimum for confidential records maintained on-line, a data base element selection process for identifying various fields of record, or various records in a file, will be applies.

System hardware and software should contain mechanical controls to insure that all on-line data inquiries and machine-generated reports will contain only the information which each user is authorized to

obtain.

System software shall be implemented to erase and clear automatically all media for the storage of data when purging is required.

PHYSICAL SECURITY

All criminal justice agencies will adopt adequate procedures for controlling physical access to manual filing areas and remote terminals and the computer facility by staff, maintenance, personnel, and visitors. These procedures may include but not be limited to the use of guards, keys, badges, access restrictions, clearance systems, sign-in logs, and similar controls.

Access to computer rooms and file storage areas will be guarded by locked doors and access permission issued only to authorized personnel. The control of access to the computer room will be effectively administered by the responsible computer center and kept in force on all shifts. Visitors must seek permission from the disseminating agency before gaining access into the computer room. Upon entry, the visitor will be given a badge to wear for identification. A log book will also be maintained for both entry and exit by visitors.

All persons having access to the rooms where criminal justice records are kept, including the locations of the remote terminals, will be properly identified and "need to be present".

Physical security measures which store criminal history record information will include but not be limited to: (1) the installation of

a highly efficient fire protection system; (2) strict control of access through locked doors; (3) implementation of storage media control procedures; (4) storage of crucial data files in a fire-proof locked vault; (5) enforcement of tight security measures and (6) establishment of backup and recovery procedures.

Recovery and Backup:

Under a computerized system in the area of computer recovery, a compatible backup computer will be designated either within the organization or in an outside facility to take care of essential daily processing in the event of severe computer malfunction or damage requiring extensive repairs.

In the area of software recovery, backup copies will be maintained in a secure location for all systems and crucial applications software and key data files. Also, a current set of the more critical data files will be maintained together with a copy of computer programs and related documentation at a remote location away from the computer room.

INDIVIDUAL ACCESS AND REVIEW

Every criminal justice agency on Guam will provide for the right of access and review. Generally, this right has not been provided for, either formally by statute or general orders and policy. Therefore, Guam must develop and formally implement via statute or executive order a policy of access and review procedure's applicable to each criminal justice agency maintaining criminal history information.

These procedures will be operational on or before December 31, 1976. The exact procedures for access and review should be completed by December 1, 1976 and will be submitted to LEAA as an addendum to this plan.

The Central Repository is scheduled for implementation approximately June 1, 1977. With the establishment of the Central Repository, procedures and mechanics of access and review will change. At that time the complete criminal history record will be available at one location.. Any procedural changes required at that time will comply with the regulations and will enhance, and make more expedient, the procedures to be implemented on or about December 31, 1976.

The individuals will only be able to get parts of their complete criminal history at the various criminal justice agencies. Because there is no Central Repository at this time, the individual agencies will maintain only that data that falls within their jurisdiction. The Guam Department of Public Safety does, however, receive dispositions back from the Attorney General's Office.

For that reason, posters will be placed at each pertinent agency, in a conspicuous place, specifying exactly what data is available at each respective agency, what procedure is to be followed to get additional data from other agencies, the hours that this service is available, and any fees for the service.

Generally speaking, the data available for review will be objective, verifiable, accurate and complete. An individual may pursue his

entire formal file at the police departments. All such requests to do so must be in writing and be approved by the Officer-in-Charge of the Records and Identification Division.

The following suggested statute addresses the availability of records for inspection within the courts and prosecuting attorney's office.

Public Records; available for inspection; cost of copies.

All public records shall be available for inspection by any person during established office hours unless public inspection of such records is in violation of any other territorial or federal law provided that, except where such records are open under any rule of court, the attorney general may determine which records in their offices may be withheld from public inspection when such records pertain to the preparation of the prosecution or defense of any action or proceeding, prior to its commencement, to which the territory is or may be a party, or when such records do not relate to a matter in violation of law and are deemed necessary for the protection of the character or reputation of any person.

Certified copies of extracts from public records shall be given by the officer having the same in custody to any person demanding the same and paying or tendering 10 cents per page copy.

There is no specific statute concerning access and review as it relates to corrections. As mentioned earlier in this plan, the CJIC Committee will develop legislative requirements for total compliance with the regulations. The information available for review has not been formulized or standardized by legislation, general orders, or documented departmental policies.

Any individual wishing to review criminal history data must verify his identity. Verification may be by fingerprints. Where feasible, this will be the procedure to be followed.

The following is a general regulatory scheme regarding requests by outside agencies for criminal history information and the fee for copying service.

"Requests by Outside Agencies"

1. Information relating to the criminal background of any individual shall be released only to government agencies within the Criminal Justice System. Data shall be disseminated on a "need-to-know" basis.

2. Representatives or authorized agents of all such government agencies shall be required to present appropriate credentials prior to having access to any information and shall not be permitted to search or have direct access to the files at any time.

3. Criminal offender record information or clearances shall be released for the purpose of securing employment only when required in the interest of national security, via an agent of the Federal agency conducting an investigation of individuals requiring top secret clearance in cases of sensitive categories, or as otherwise required herein.

4. When such information is required in the interest of national security, the requesting agent shall certify that the individual being investigated is an applicant or employee in a position which requires a top secret clearance.

Fees:

1. A fee of fifty (50) cents shall be charged for each "Abstract of Criminal Record" and twenty-five (25) cents for each copy thereafter.

2. A fee of fifty (50) cents shall be charged for a letter of clearance and twenty-five (25) cents for each copy thereafter.

3. No charge for services rendered to a government agency.

An individual should be given a document copy only when it is the intention to register a formal challenge that the document

contains erroneous data and the copy is required to adequately prepare the challenge. It is the desire of the territory and all relevant agencies to maintain the highest degree of accuracy in all files containing criminal history data. For this reason the forms and procedures for challenge will be designed in as simple and straightforward a manner as possible.

Each agency, as part of the certification and agreement, will specify a department within the agency responsible for conducting administrative reviews of all challenges. In the event that the challenge of erroneous data is well founded, the errors will be corrected and a list of non-criminal justice agency or individual recipients of the erroneous data will be provided. If it is the best judgment of the challenged agency that the data is not in error, the individual will be notified of that decision. The individual has the right to appeal that decision.

The CJIC Committee will be responsible for the preliminary arbitration. Should the appeal not be resolved by the CJIC Committee, it will then be sent to the Attorney General's Office for a final decision.

Section 3

RESPONSIBILITIES OF INVOLVED AGENCIES

This section of the plan addresses the responsibilities of all agencies involved in the successful implementation of the plan. These responsibilities may be redundant with topics discussed elsewhere in the plan; however, they are repeated here for clarification.

The implementation of this plan will be a collective effort by several different agencies. Each agency will assume the appropriate position that falls within its technical charter or that it is legislatively responsible for by virtue of existing statutes. Where the responsibility is not clear, specific legislation will be pursued. In the interim and for the sake of expediency, the following responsibilities have been assigned.

CRIMINAL JUSTICE INFORMATION CENTER (CJIC)

The CJIC will have the overall responsibility for the collection, storage, or dissemination of criminal history record information. This plan addresses that authority that extends its responsibility to encompass the following activities:

(1) Managerial control over the Central Repository.

(2) Monitoring compliance with the restrictions set out in the regulations.

(3) Development and implementation of annual audits and quality control procedures to ensure compliance with the regulations. These audits will address the collection, storage, and dissemination of criminal.

(4) History information.

ATTORNEY GENERAL'S OFFICE

(1) Preparation of formal agreements, and notices to be entered into between disseminating and recipient agencies.

TERRITORIAL CRIME COMMISSION (TCC)

As the State Planning Agency, TCC will be responsible for monitoring all future grants to ascertain appropriate plans for compliance with the privacy and security regulations.

THE CRIMINAL JUSTICE INFORMATION CENTER COMMITTEE

The responsibility of this committee was discussed supre in the introduction. Essentially, it will provide policy, review and appeal, and propose legislation and executive action to implement the federal regulation.

POLICY/ADVISORY GROUP ON CRIMINAL JUSTICE COMPUTER INFORMATION SYSTEM

This group, which will oversee the feasibility study (discussed upon) of implementing a computerized criminal justice information system, and will provide a detailed and exact plan, which will implement the secutiry and privacy plan of the federal regulation into a computerized system.

ALL OTHER AGENCIES GOVERNED BY THE REGULATIONS

All other agencies will, under the authority and direction of the Attorney General, comply with the regulations of privacy and security. This compliance encompasses privacy and secondary dissemination of criminal history information, the execution of appropriate agreements

and notices relevant to dissemination, receipt and usage of such data, and all other requirements concerning the storage and maintenance of such data. In addition, the right of access and review policy shall be implemented according to the procedures presented in this plan.

Section 4

IMPLEMENTATION MILESTONE SCHEDULE

The implementation schedule is contingent on Guam's territorial legislature appropriating local matching funds for the 1977 FY request of $120,000.00 for a feasibility study of developing a computerized system for the collection, storage, and dissemination of criminal justice history. Since the Guam legislature will not reconvene in session until June, 1976, the following important milestones have been identified and are scheduled under the assumption that Guam's legislature will appropriate the necessary matching funds in June. Any amendments of said schedule will be submitted as an addendum to this plan.

Activity	Milestone Date
Central Repository established	June 1, 1977
Access and Review Procedures established and implemented	December 31, 1976
Certification Process complete	December 31, 1976
Agreements and Notices developed	December 31, 1976
Sanctions for Non-compliance established	December 31, 1976
Privacy Committee formed	June 1, 1977

Section 5

PART A

The power of information systems to compile data on individual citizens is unlimited. If such systems are to obtain the respect of the citizenry and receive popular support for their continued use as a tool in the administration of justice, those who operate these systems must respect the limited purposes for which they are created.

The important area of security and privacy concerns the need to maintain a balance between the necessity of the criminal justice community for information about its clients and the right of the individual to privacy. Issues raised concern distribution of information, scope, accuracy, and timeliness of information, as well as protecting information from unauthorized tampering or destruction.

The regulations proposed are minimum standards for criminal justice information systems. They are not intended to cover all the exigencies which may arise in the development of a particular system, nor should they prevent any one system from adopting more strict regulations. In short, they can be (and may need to be) supplemented or tightened; but not circumvented.

PRIVACY COMMITTEE

A.1 A Privacy Committee shall be created to coordinate these regulations. The committee shall be composed of representatives of criminal justice agencies, information systems, and the general public.

A.2 The Privacy Committee shall have the responsibility to recommend modification of these regulations, so far as consistent with applicable law.

A.3 The Privacy Committee shall have the responsibility to impose non-penal sanctions for agencies which fail to comply with these regulations.

A.4 Every criminal justice agency participating in a criminal justice information system shall appoint one person to be responsible for compliance with these security and privacy regulations.

PART B

ACCESS

To protect confidentiality of information in criminal justice manual file and data banks, rules must exist which govern access to and the sharing of either system. The general principle, followed in these regulations, is the concept of limited dissemination. Criminal justice agencies should share among themselves only that information which is relevant to their statutory responsibilities; non-criminal justice public agencies and officials should obtain data only where they have specific statutory authorization to use it.

Reports and records prepared at the request of the court in juvenile proceedings shall not be disclosed directly ... to anyone other than the judge or others entitled under this title... Guam Code of Civil Procedure Section 271.

There are strong policy reasons for adopting a public records law which restricts dissemination of criminal history data. Tension exists between the individual's rights to privacy and the public's traditional abhorrence of a public agency conducting its activities under a veil of secrecy. The records of individual occurrences, such as arrests, complaints, and convictions, are commonly recognized to be public information.

However, the same records when compiled and automated on an individual basis do not serve the function of providing the public with data for evaluating agency behavior; they provide agencies with

needed information to judge individual behavior. And, because of the inherent dangers of abuse and personal detriment, they may be justifiably restricted to those agencies which need the information for official business.

B.1 a. Criminal justice agencies means only those public agents or components thereof, at all levels of government, which, as their principal function, perform activities relating to (1) collection and analysis of crime statistics pursuant to statutory or administrative authority; (2) the apprehension, prosecution, adjudication, or rehabilitation of criminal offenders; or (3) the collection, storage, dissemination, or usage of criminal justice record information.

b. Criminal justice record information refers to information contained in a criminal justice information system. Intelligence or investigatory information maintained by one agency and not disseminated is not included unless specifically identified.

Individual record information refers to that criminal justice record information which permits identification of an individual or can be accessed by personal identifiers.

Comment: Any type of information if it does not permit identification of the individual record subject can be stored in a criminal justice information system.

c. Unless stated otherwise, the standards concern criminal justice agencies, criminal justice record information and criminal justice agencies.

B.2 Direct access to criminal justice record information shall be limited to criminal justice agencies.

B.3 Criminal justice agencies shall obtain, whether by direct access or otherwise, only that information which is relevant to their statutory responsibilities, provided that each criminal justice agency shall have access to its own files in an information system.

B.4 Non-criminal justice public agencies and officials shall obtain only that individual record information which is specifically provided for by territorial law.

B.5 No corporation, private agency, or individual shall obtain individual record information unless such dissemination is specifically provided for by law.

Comment: Private employers, security firms and investigators, credit agencies, insurance companies, and banks may attempt to obtain criminal history information on individuals, particularly where employability is concerned.

Nevertheless, this information is not a matter of public record.

B.6 Where juvenile record information is maintained by a law enforcement agency, that information may be shared only among local law enforcement agencies or upon order of the Superior Court.

It is recognized, however, that law enforcement agencies have legitimate needs to maintain records on juveniles and these records are also treated as confidential. They will be open to person whose official duties relate to the juvenile laws.

Standard B.6 interprets this section to limit dissemination, at least as applied to records and to other law enforcement agencies.

B.7 Intelligence information obtained from a criminal justice information system including the fact that an individual has an intelligence file or name of agencies that possess intelligence information on him, shall not be disseminated outside of criminal justice agencies.

B.8 In all cases where criminal justice record information is open to public inspection by law, the custodians of that information shall adopt reasonable regulations to permit public access.

B.9 No agency qualified under these regulations to obtain criminal justice record information may obtain access until it has signed a non-disclosure agreement, as adopted by the Privacy Committee.

Comment: The typical penalty for violation of a non-disclosure agreement is temporary or permanent exclusion from an information system.

B.10 Any person maintaining or receiving individual record information shall, prior to each use or further dissemination of such information, take reasonable action to assure that the information is the most accurate and complete available.

B.11 Those agencies or individuals engaged in legitimate research programs may obtain criminal justice record information for research if each agency contributing and maintaining the information consents and the Privacy Committee implements the following requirements.

a. In no case shall information furnished for purposes of any program of research be used to the detriment of the persons to whom such information relates.

b. In no case shall information furnished for purposes of any program of research be used for any other purposes; nor shall such information be used for any program of research other than that authorized and approved by the Privacy Committee.

c. Each participant and employee of every program of research authorized access to information shall, prior to having such access, fully and completely execute a non-disclosure agreement approved by the Privacy Committee.

d. In every case, the authorization for access to information shall assure the Privacy Committee full and complete rights to monitor the program of research. Such monitoring rights shall include the right of the Committee, its agents or employees to audit and review such monitoring activities and also to pursue its own monitoring activities.

B.12 It is understood that violation of these regulations may subject the individual to criminal and civil liability.

Comment: Guam does not have a criminal law specifically punishing those who may abuse or wrongfully disseminate the information in criminal record history systems.

PART C

PRIVACY

Privacy refers to the protection of the interests of the people whose names appear, for whatever reason, in the contents of a criminal justice information system. When information about an identifiable individual has been obtained by a criminal justice agency, the important consideration becomes one of confidentiality--who within or outside the agency is allowed access to a given record or file.

The following standards are based on the premise that one of the most important ways to protect the individual's rights of privacy in an automated system is to limit the information which the system may possess. The standards prescribe strict rules regarding information quality and completeness. An additional safeguard is the right of the individual to inspect his own record for inaccurate or misleading statements.

C.1 Individual record information shall be objective, verifiable, accurate, and complete. In following this standard:

a. Individual record information which is anecdotal, evaluative, or judgmental shall not be computerized; provided that where an agency's responsibilities require behavioral analysis of individuals, that agency may automate standardized personal evaluation data entries of a type useful for research classification.

Comment: One of the most serious public complaints about individual data banks is that they will computerize for indefinite periods such soft social-work type of evaluations as "drug problem" or "suicidal tendencies." For this reason, it is generally agreed that criminal histories will not contain behavorial data. Standard C.1a recognizes, however,

that some correctional agencies will want to contain certain individual analysis. The standard requires use of a uniform vocabulary based, insofar as possible, upon widely accepted behavorial terms.

b. Individual record information that arrest took place or prosecution was initiated shall not be disseminated without inclusion of a final law enforcement or judicial disposition; provided that, until a final disposition is reported but not longer than two years, "disposition pending" may be utilized.

c. Individual record information in intelligence filed subject to access by an agency which did not originate the information shall be limited to personal identifiers and such data as is available from sources open to public inspection. Intelligence files may also identify law enforcement agencies possessing additional intelligence information relating to such individuals.

C.2 Individual record information entered in a file shall be relevant to the purpose for which the file was created. In following this standard:

a. Misdemeanor drunk and traffic records where the case did not result in imprisonment or probation supervision shall not be entered in criminal history filed.

b. Misdemeanor or felony arrests not leading to conviction shall not be entered in criminal history files unless the individual has prior convictions or is a fugitive from justice.

Comment: Several recent cases have raised the issue of whether the constitutional right to privacy or equitable grounds of fairness permit a criminal justice agency to maintain records on persons whose arrests did not lead to conviction. The results are not conclusive.

In Menard v. Mitchell, 328 F.Supp 718 (D.C.Cir.1971), the U.s. District Court found that arrest records which showed release without further prosecution might still

be useful to law enforcement agencies; the court prohibited, however, dissemination to non-criminal justice agencies. On the other hand, the Washington Court of Appeals found that the constitutional right of privacy overrode the police necessity to keep the fingerprints and photos of an acquitted person. Eddy v. Moore, 487 P2d 211 (Ct App 1971). And the Colorado Supreme Court held that the retention of arrest records of an acquitted person without justification from the standpoint of law enforcement or creation of methods to insure record confidentiality may constitute an invasion of privacy. The court recognized the significance of the "computer age" in bringing record-keeping issues to the public's attention. Davidson v. Dill, 503 P2d (Colo Sup Ct 1972).

C.3 Individual record information relating to juvenile shall be maintained separately from that relating to adults.

C.4 Individual record information in intelligence records relating to organized crime and racketeering activities shall be maintained entirely separately from civil disorder/subversive activities record information.

Comment: This regulation is proposed as a matter of practicality. Civil disorder files involve constitutional questions of great seriousness. Such questions are only beginning to reach courts and legislators and to affect public attention. If such files are intermingled with organized crime intelligence records, the constitutional problems implicit in the former would inevitable attach to the latter. In addition, the political and public acceptance of organized crime intelligence systems may be crowded by the controversy that surrounds civil disorder files.

C.5 Individual record information shall not be disseminated unless the requesting agency is able to identify the record subject by a specified set of personal characteristics.

Comment: In some systems, fingerprints are an available means to safeguard against mistaken identity. Where use of fingerprints is not feasible, some other set of personal identifiers must be required.

C.6 Every individual, his attorney of record, and his parents or guardian, if a minor, shall have the right to examine all individual record information which refers to him.

a. This right of examination shall encompass the computer log of agencies which have requested

access to the individual's record.

b. This right of examination shall be subject to reasonable procedures, to be established by the Privacy Committee.

c. Any individual who believes that individual record information which refers to him is inaccurate or misleading may petition the Privacy Committee for additions to, deletions from, or comments upon the record information.

d. Notice shall be clearly given or posted in criminal justice agencies concerning the laws and conditions under which an individual may view and correct his criminal offender record.

Comment: The right of an individual to inspect his own record can be an important safeguard. Such inspection does not interfere with criminal justice use of the records and it provides an additional guarantee of accuracy in the information reported. Juveniles, of course, are already accorded this right under juvenile court law.

In common practice, the individual is permitted to see his own record and take notes, but not to obtain a copy. The purpose of this approach is to make it impossible for employers to condition employment on production of the actual rap sheet.

PART D

RECORD RETENTION

Criminal justice information systems require guidelines on how long records should be maintained. There are two general reasons behind the rules for purging files with information on individuals. One is to eliminate information which, because of its age, may be an unreliable guide to the subject's present behavior or situation. The second is somewhat more philosophical. There exists a point in time after which it only seems fair to give individuals a fresh start. It is difficult to judge, of course, when that point is reached.

For records, such as cases in progress, which do not store data on individuals, a general rule is that the file should be purged when it is no longer required or useful. Such action is required to keep the computer system at maximum efficiency.

The most difficult problem is determining how long to maintain criminal history information on an individual. In some systems, the practice is to keep records until it is likely that the individual has died. Such policies violate both of the concepts underlying reasonable, realistic retention rules. Both the probity of the records and the stigma attached to them may terminate for many individuals at an earlier point, especially since the average adult criminal is relatively young.

Guam law contains no guidelines for purging criminal histories.

One national body composed of representatives from the entire spectrum of criminal justice has proposed that 10 years free of subsequent criminality for felons and five years misdemeanors is a reasonable and fair standard.

D.1 a. Reasonable rules for routine purging of individual record information shall be established. In following this standard.

b. Information for keeping track of an individual as he proceeds through the criminal justice system shall be purged within three months of the individual's exit from processing. This rule applies to correctional files and case-in-progress files which are essentially on-line and available for interagency sharing.

c. Information in criminal history files on an individual convicted of a misdemeanor shall be purged when the conviction and release from supervision is at least five years earlier, provided there have been no subsequent criminal convictions.

d. Information in criminal history files on an individual convicted of a felony shall be purged when the conviction and release from supervision is at least 10 years earlier, provided there have been no subsequent criminal convictions.

e. Information in criminal history files related to an offense for which an individual has been pardoned shall be purged upon notification.

f. Information in criminal history files subject to an expungement order shall be purged upon notification.

g. Purging requires that information be destroyed or stripped of personal identifiers.

D.2 Whenever a minor exceeds the jurisdictional age of the Juvenile Court:

a. All juvenile record information relating to the minor which has been maintained by a Juvenile Court shall be physically removed; and

b. All juvenile record information relating to the minor which has been maintained by a law enforcement agency shall be destroyed.

D.3 Whenever juvenile information is physically removed pursuant to these regulations, storage and use of the information shall be the direct responsibility of the Juvenile Court.

Comment: Under this regulation, the Juvenile Court retains its statutory authority to govern dissemination by court order on a case-by-case basis. Guam Code of Civil Procedure, Sections 271 and 271.1.

Juvenile records are traditionally accorded a great degree of confidentiality. For this reason, it is recommended that, once the minor reaches adulthood, the record be maintained in a central repository, thus permitting substantial control over its dissemination.

PART E

SECURITY

No information system will ever be completely safe from unauthorized alteration, removal, or destruction of information. Nevertheless, such systems can be made reasonably secure through a combination of technical, physical, and personnel measures. Information system security is the capability to restrict the availability of specific information to authorized individuals, and to physically protect all parts of the system, including both the data and the system that processes the data, from any form of hazard that might endanger its integrity or reliability.

While the following regulations represent standards which all information systems and data processing centers should adopt, in the final analysis the implementing agencies must decide the rights of individuals. In each case, an estimate of the cost or probability of the threat must be weighed against the use of providing adequate information system security.

E.1 Terminal and Operator Identification.

a. There shall be a terminal identification code number for each remote terminal as a precondition for entering the files.

b. Within each agency, terminal use shall be assigned to a limited and identified group of individuals.

Comment: Most often, persons having access to a file have access to all fields of all records. In a manual file where records are maintained in a manila folder, it is difficult to do otherwise.

In a computerized system, however, access can be permitted to the entire file or restricted to certain fields of the file. For example, access rights might be to:

(1) Read an item (e.g., file, record, or field)

(2) Write an item so as to produce a change--either;

  (a) a new item added, or
  (b) an existing item changed

(3) Delete an item.

The access rights of a user must be explicitly denoted in any situation where partial rights exist, e.g., for a limited access file or where reading is permitted but changes and deletions are not. It is recommended that an authorization table (or matrix) be stored with the data and their access rights. Access to this table must be strictly limited to persons authorized to modify the table and be stored separately from the data.

c. Each individual terminal user shall identify himself by a personal identification number.

Comment: For particularly sensitive data, such as intelligence information, a callback procedure may be instituted, in additional to the recognition of the personal identification number, to authenticate the identity of users requesting confidential data from remote terminals.

d. The computer shall be programmed to log the identity of all users, the files accessed, and the date of access. This information shall be maintained for 12 months.

e. Each remote terminal user shall establish a written log of terminal use as required by the Privacy Committee, which shall be audited periodically.

Comment: In systems which transmit criminal history information, the written log of terminal use is an acceptable safeguard for determining instance of unauthorized file access. This standard is intended to give the Privacy Committee the authority to determine for which criminal history files and in what access situations the written log would be a useful protection.

The standard is not intended to apply to situations where most of the data to be transmitted is management information belonging to the terminal user. In that instance, the requirement of a written log could be in onerous burden.

E.2 Protections against Wiretapping, Eavesdropping, or other Forms of Non-Terminal Interception.

Adequate measures shall be established through hardware and software features to protect against unauthorized non-terminal interception.

Comment: Non-terminal interception involves an attempt to obtain information transmitted by the computer through wiretapping or electromagnetic pick-up. Wiretaps are feasible whenever a system uses calbes to connect components; electromagnetic pick-up requires capturing the radiated signals emanating from the computer and its communication lines.

The methods used for non-terminal interception are not capable of altering or deleting information in a computer file but the risk does exist that messages will be recorded as they are sent or received. Since this risk varies with the size of the system and the nature of the messages, there is no one recommended way to minimize it. For this reason, each system should determine what measures it wishes to employ at different stages during the growth of systems.

One generally recognized deterrent is to code or scramble data during transmission. The receiving terminal decodes the message so that it becomes coherent upon receipt.

A second method is to shield the computer and communications lines so that electromagnetic emanations cannot be captured. Where the data is coded, the shield system is not necessary unless there is a serious possibility that the intercepter can decode the data.

E.3 Data Storage.

a. Data shall be stored in a data classification system according to scope of permitted access and sensitivity of the data.

Comment: A basic data classification system for criminal justice information systems is provided in Standard 8,5, "Data Sensitivity Classification" of the National Advisory Commission of Criminal Justice

Standards and Goals, Report on the Criminal Justice System (1973).

b. Confidential criminal justice records that are maintained on-line in a time-shared, remote access computer system should be either password protected or have some form of inscription that at least prevents accidental disclosure, or both.

Comment: Passwords, in addition to a personal identification number, can serve for authentication of a user's identity or can be used to authenticate the authorization of a user to access a file. Passwords should be subject to change as often as wanted by the user.

As a general rule, the more sensitive the data the more complex should be the inscription for transmission purposes. As a minimum for confidential records maintained on-line, a short key transformation for identifying various fields of a record, or various records in a file, should be applied.

c. System hardware and software shall contain mechanical controls to insure that all on-line data inquiries and machine-generated reports will contain only the information which each user is authorized to obtain.

Comment: A file reader program of an operating system should be used for access to all files that are made accessible on a field-limited basis.

d. System software shall be implemented to erase and clear automatically all media for the storage of data when purging is required by these regulations.

e. Duplicate computer files shall be created as a countermeasure for unauthorized destruction of original files and all computer tapes or discs shall be locked in a safe storage area under the control of senior agency personnel. Secondary storage may be used for backup.

Comment: For the purposes of record retention, duplicate computer files or backup files should be treated in a similar manner as the original files. In this way, record retention schedules can apply uniformly to all computerized records as well as related records in secondary or backup storage.

E.4 Data Entry.

a. The Privacy Committee shall have the authority to require that a specific data element which fails to satisfy the standard of objectivity, verifiability, accuracy, or completeness shall be excluded or deleted from individual record information.

b. Where data is submitted to a computer center on reporting forms, the data center shall establish procedures for destroying these forms or storing them in a secure environment after data is entered in the computer.

c. System software shall contain controls to insure that each terminal is limited as to the information it can input, modify, or cancel in accord with the personnel authorization table and the data classification system.

E.5 File Protection Software.

a. Procedures shall be created to disconnect any remote terminal whenever repeated errors indicate that tampering is taking place.

b. A monitor program shall be developed to report attempts to penetrate any system, program, or file.

c. Edit programs shall be created to periodically audit record alteration transactions.

d. All file protection software shall be written, installed, and stored by the systems management and technical personnel who are under the management and control of the implementing criminal justice agency. Records of these programs shall be stored under maximum security conditions. No other persons, including staff and repair personnel, shall be permitted to know these programs.

Comment: The concept underlying this standard is that all sensitive software shall be prepared by a limited number of criminal justice agency personnel. All activities related to these programs shall be performed by these personnel only.

E.6 Physical Security.

a. All criminal justice agencies will adopt adequate

procedures for controlling physical access to the filerooms or computer facility and remote terminals by staff, maintenance personnel and visitors. These procedures should include the use of guards, keys, badges, access restrictions and clearance systems, sign-in logs and similar controls.

Comment: As a general rule, all persons having access to the rooms where records are kept, including the locations of the remote terminals should be properly identified and "need to be present."

b. Data centers will design site preparation and configuration to facilitate maximum security measures.

E.7 Employee Security.

Data centers shall adopt regulations for the hiring, retention, and continual training of personnel.

Comment: Anyone who is entrusted with access rights to data is a potential security leak for that data. The most direct method of access for an intruder is through a person in a position of trust. This problem is well known, particularly within law enforcement agencies, and many methods are used to decrease the probability of a betrayal of trust. Personnel are investigated to determine trustworthiness, stability, and freedom from behavior that might lead to their being compromised. It should be made explicit what the penalties are for breach of trust, so that there will be a deterrent against disclosing confidential information. In addition, the chance of accidental disclosure should be minimized by having security procedures with regard to labeling of sensitive data, locking of file cabinets, etc. The problems here are identical with those of security of data in a manual system.

The following represent analogous standard for security of manual files.

E.8 Identification.

a. Badges, visitor passes, or other similar identifiers is required as a precondition for entering the record and filing area.

b. Within each agency, use of criminal history records and files shall be limited to a specific and identifiable group of individuals.

c. Access rights of a user must be explicitly denoted in any situation where partial rights exist, e.g., for a limited access file or where reading is permitted but changes and deletions are not.

d. An authorization table must be kept by each agency deliniating user's access rights. Access to this table will be limited to persons authorized to modify the table.

e. The Central Repository shall log the identity of users, the files accessed, and the date of access. This information shall be maintained for 12 months.

f. Each user agency shall establish a written log of all users, files accessed, and the date of access. Logs shall be audited periodically.

E.9 Storage.

a. Files shall be stored and classified in a system according to the scope of permitted access and sensitivity of the records.

b. Purging shall be accomplished as required by these regulations.

c. Duplicate files shall be maintained as a countermeasure for unauthorized destruction or tampering with original files.

Comment: It is suggested that microfilm be utilized for the purpose of duplication.

E.10 Record Entry.

a. The Privacy Committee shall have the authority to require that a specific record element which fails to satisfy the standard of objectivity, verifiability, accuracy, or completeness, shall be excluded or deleted from individual record information.

b. Where information is submitted on reporting forms, the center shall establish procedures for destroying these forms or storing them in a secure environment after said information is entered in the master file.

Comment: Anyone who is entrusted with access rights to data is a potential security leak for that data. The most direct method of access for an intruder is through

a person in a position of trust. This problem is well known, particularly within law enforcement agencies, and many methods are used to decrease the probability of a betrayal of trust. Personnel are investigated to determine trustworthiness, stability, and freedom from behavior that might lead to their being compromised. It should be made explicit what the penalties are for breach of trust, so that there will be a deterrent against disclosing confidential information. In addition, the chance of accidental disclosure should be minimized by having security procedures with regard to labeling of sensitive data, locking of file cabinets, etc. The problems here are identical with those of security of data in a manual system.

Section 6

CERTIFICATION PROCESS

An integral part of Guam's Plan to implement the Department of Justice's rules and regulations governing criminal history information is the certification statement. Guam's plan for accomplishing this certification will be completed by each and every agency which must comply with the rules and regulations. A certification checklist form will be designed that will be able to meet the needs of all the agencies involved and meet all of the requirements of the rules and regulations in regards to completeness and accuracy, limits on dissemination, audits and quality control, security, and individual rights of access and review.

Initially, a cover letter explaining the ramifications of the new rules and regulations, and a copy of the rules and regulations will be sent to each concerned agency. Staff members of the Center will follow up these initial letters by direct contact with all the agencies. This contact, whether it be in person or by telephone, will be for the purpose of responding to any questions that may arise.

Once all remaining questions have been resolved, arrangements will be made by the CJIC staff to meet with appropriate representatives of the criminal justice agencies involved in order to distribute and complete the certification checklists.

At present, pending the appropriation and allocation of funds for FY 1976 for a feasibility study of a computerized system of criminal record history collection, storage, and dissemination, none of Guam criminal justice agencies fall into inclusion under the federal regulation. Therefore, in anticipation of this appropriation being allocated, CJIC will prepare the mechanics for the certification process.

LAW-ENFORCEMENT

Department of Public Safety

PROSECUTION

Attorney General's Office

ADULT CORRECTIONAL INSTITUTIONS

Guam Penitentiary, Community Correctional Center

JUDICIAL

Superior Court of Guam
Supreme Court of Guam

PAROLE

Territorial Parole Board

The probation function falls within the judiciary.

Section 7

DEVELOPMENT OF CRIMINAL JUSTICE INFORMATION CENTER (CJIC)

In collecting, storing, and disseminating criminal history record information, CJIC must insure that all criminal history record transaction are complete and accurate.

The Guam CJIC will be housed at the Department of Public Safety's Records and Identification Bureau. However, before this bureau can fulfill the function of a central repository it must first be upgraded in training, equipment, and additional personnel. This upgrading can only be achieved through allocation of additional or supplemental funds to finance an operational central repository.

The costs to improve the Records and ID Bureau is itemized as follows:

EQUIPMENT		
Microdisc System		68,000.00
Microdisc System Spare Parts		27,000.00
Desks, 4 pedestal	@ 167.14 -5 each-	835.70
Desks, Typing	@ 186.72 -3 each-	560.16
Chairs, Typing	@ 36.29 -3 each-	108.87
Chairs, Swivel	@ 39.32 -5 each-	196.60
Typewriters, electric	@ 645.84 -3 each-	1,937.52
Air Conditioners	@ 400.00 -2 each-	800.00
Classification Magnifying Glass	@ 5.00 -5-	25.00
		99,463.85

PERSONNEL

Clerk Typist II	-3- @ 6604	24,000.00
Fingerprint Classifiers	-5- @ 7628	50,000.00
Microdisc Operator	-1- @ 7628	10,000.00
		84,000.00

CONTRACT SERVICES

Microdisc System Maintenance	-1 year-	4,000.00
Microfilm Camera Rental	-1 year-	1,500.00
Film Processing Costs	-1 year-	1,500.00
Microdisc Systems Engineer	-3 months-	20,000.00
Office Space Rental (1000 sq. ft.)	-1 year-	4,500.00
		31,500.00

TRAINING

Microdisc Operator

Travel - 850.00

Per Diem 490.00
1,340.00 1,340.00

Supervisor, Fingerprint Classifier (LAPD)

Travel - 850.00

Per Diem 490.00
1,340.00

Equipment	99,463.85
Personnel	84,000.00
Contract Services	31,500.00
Off-Island Training	2,680.00
	217,643.85

90% 217,643.85 = 195,879.47

10% 217,643.85 = 21,764.39

Note that the total costs involved are presently inflated by ten percent. However, the overall costs may be mitigated by the Department of Public Safety providing within its own budget for some of the personnel and equipment necessary for a CJIC operation.

It is envisioned that a microdisc system will be utilized for fingerprint classification and identification. Such a system will be essential to the respository since the verification of identity will be by fingerprinting. As a fundamental rule, fingerprints will govern the entry of data into a criminal history file. Commensurate with the utilization of the microdisc system are the itemized expenses under CONTRACT SERVICES and also the necessity of training a microdise operator.

Generally, it can be stated that an operational CJIC will not evolve unless the requested funding is met. Without sufficient appropriations, it is doubtful that a CJIC can be implemented and without the CJIC, the overall objectives of a criminal history record information system will be unattainable.

It is encouraged, therefore, that the territorial government place the funding of this venture on the highest priority.

ADMENDMENTS

TO

PRIVACY AND SECURITY PLAN

- 0 -

June 16, 1976

AMENDMENTS TO THE PRIVACY AND
SECURITY PLAN OF THE TERRITORY OF GUAM 6/16/76

Page 2-7

First paragraph under Limits On Dissemination

Delete the word "specific" in the sixth line of first paragraph.

Page 2-32

Add under "Requests by Outside Agencies"

5. Criminal history record information shall be released for purposes of international travel (issuance of visas) and granting of citizenship.

Page 5-3

First Paragraph

Delete the word "specific" in the last sentence, last line of first paragraph.

Page 5-4

Add to paragraph B.1, part d which provides:

d. "Nonconviction data" means arrest information without disposition if an interval of one year has elapsed from the date of arrest and no active prosecution of the charge is pending; or information disclosing that the police have elected not to refer a matter to a prosecutor, or that a prosecutor has elected not to commence criminal proceedings, or that proceedings have been indefinitely postponed, as well as all acquittals and all dismissals.

Page 5-5

Delete from paragraph B.4 the word "specifically" so that sentence will read as follows:

Non-criminal justice public agencies and officials shall obtain only that individual record information which is provided for by territorial law.

Delete from paragraph B.5 the word "specifically" so that the sentence will read as follows:

No corporation, private agency, or individual shall obtain individual record information unless such dissemination is provided by law.

Also delete from paragraph B.5 the last sentence:

> Nevertheless, this information is not a matter of public record.

and add in its place:

> The territory will determine the purposes for which dissemination of criminal justice records is authorized by law, executive order, court rule, decision, or order.

Redesignate paragraph B.8 as B.8 (a) and add the following paragraphs to be designated B.8 (b) and B.8 (c).

B.8 (b) A criminal justice agency shall disclose to the public criminal history record information related to the offense for which an individual is currently within the criminal justice system.

B.8 (c) A criminal justice agency shall confirm prior criminal history record information to members of the news media or any other person, upon specific inquiry as to whether a named individual was arrested, detained, indicted, or whether an information or other formal charge was filed, on a specified date.

END