Privacy and Security of Criminal History Information

A GUIDE TO ADMINISTRATIVE SECURITY

National Criminal Justice Information and Statistics Service
Law Enforcement Assistance Administration
U.S. Department of Justice
Washington, D.C. 20531

U.S. Department of Justice
Law Enforcement Assistance Administration

James M. H. Gregg
Acting Administrator

Harry Bratt
Assistant Administrator
National Criminal Justice Information
and Statistics Service

Carol G. Kaplan
Director, Privacy and Security Staff

Document prepared by THEOREM Corporation pursuant to LEAA Contract J-LEAA-0342-8.

Privacy and Security of Criminal History Information:

A GUIDE TO ADMINISTRATIVE SECURITY

National Criminal Justice Information and Statistics Service
Law Enforcement Assistance Administration
U.S. Department of Justice
Washington, D.C. 20531

For sale by the Superintendent of Documents, U.S. Government Printing Office
Washington, D.C. 20402

Stock No. 027-000-00738-4

Preface

This guide describes, in general terms, those requirements of the LEAA Regulations governing privacy and security of criminal history information (28 CFR Part 20) which pertain to administrative security. It is intended that the document clarify both the obligation and authority of criminal justice agencies as well as the responsibilities of non-criminal justice agencies and private companies whose work is associated with criminal history information.

This document represents the third in a series of guides prepared by the Privacy and Security Staff, National Criminal Justice Information and Statistics Service (NCJISS), to discuss individual requirements of the Regulations. The initial two publications, "Privacy and Security of Criminal History Information: A Guide to Dissemination," and "Privacy and Security of Criminal History Information: A Guide to Review and Challenge" are available through the National Criminal Justice Reference Service. "A Guide to Audit Procedures" will be released in the near future. Further information regarding these materials can be obtained by contacting the Privacy and Security Staff, NCJISS; LEAA, Washington, D.C. 20531.

Background

The Statute

The Department of Justice–Law Enforcement Assistance Administration Regulations which govern the privacy and security of criminal history information systems (28 CFR Part 20) implement Section 524 (b) of the Omnibus Crime Control and Safe Streets Act of 1968, as amended.

This section was added to the Act in August, 1973. It provides that:

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

The Regulations

Section 20.21 (f) of the LEAA Regulations (28 CFR Part 20), as published on March 19, 1976, describes, in general terms, the administrative, computer, and physical security requirements to ensure the confidentiality and integrity of criminal history information. These are to be implemented consistent with standards and procedures established in each state either by legislation or Regulations as appropriate.

Original provisions defining Security requirements were included as part of the Regulations which were initially published on May 20, 1975. The major impact of these original provisions was to require that criminal history information be stored only in computers that were "dedicated" to criminal justice activities. This really meant that only computers operated by criminal justice agencies would qualify. In recognition of strong opposition to this position, LEAA reopened this section of the Regulations to hearings and, on the basis of testimony received therein, amended the Regulations to delete the "dedication" requirement.

Administrative Security Requirements

In general, those sections of the Regulations which deal with administrative security require that procedures be adopted to ensure:

—that access to criminal history information system, data, facilities, operating environments, data file contents, and systems documentation is restricted to authorized organizations and personnel.

—that any individual or agency authorized direct access to criminal history information is made responsible for (1) the physical security of criminal history information under its control or its custody, and (2) the protection of such information from unauthorized access, disclosure, or dissemination.

—that each employee working with or having access to criminal history information is made familiar with the substance and intent of these regulations.

—that a criminal justice agency will screen (review employee applications) and have the right to reject or, in a shared computer facility, request alternative assignment of individuals who will be authorized to have direct physical access to criminal history information. (Rejection to be based on good cause and should be in accordance with written standards for such employment.)

—that a criminal justice agency shall have the right to initiate (or in the case of a shared system, cause to be initiated) administrative action leading to the transfer or removal of personnel who have direct access to such information when such personnel violate the provisions of these Regulations or other security requirements established for the collection, storage, or dissemination of criminal history information.

— that where a computerized criminal history system is operated by a non-criminal justice agency, the criminal justice agency shall obtain the authority (normally by written contract between the criminal justice agency and the non-criminal justice agency, a sample of such agreement is set out on page 25) to develop or approve the procedures and techniques for the security of those portions of the system that include criminal history information (in accordance with standards established by the Regulations), and to audit, monitor, and inspect such procedures and techniques.

Computer Security/Physical Security Requirements

In general terms, those sections of the Regulations which refer to "computer" and "physical" security require that procedures be developed and/or approved by a criminal justice agency to ensure:

—that computerized criminal history information can only be input, accessed, purged or otherwise modified by authorized criminal justice controlled terminals.

—that operational computer programs are utilized to prevent, detect and record unauthorized attempts to penetrate the criminal history information system.

—that the above programs are known only to persons who are cleared to work with criminal history information.

—that any central repository, whether manual or automated, is physically protected against unauthorized access, theft, sabotage, fire, flood, wind or other natural or man-made disasters.

The Regulations apply to both manual and computerized criminal history information systems and do not require that information be stored in a "dedicated" criminal justice computer system.

Impact

The administrative security requirements, in general, can be implemented by criminal justice agencies without significant new expenditures of funds or other formal modification of established policies. Members of the criminal justice community have traditionally been aware of the need for security of records and information, and the Regulations on administrative security generally reflect agreed-upon standards of care. One benefit to criminal justice agencies is that the Regulations provide a clear basis for establishing a contractual relationship where criminal justice data processing services are to be provided by a non-criminal justice agency. This is the case since the Regulations explicitly state that authority for development and/or approval and audit of security standards impacting on criminal history information must reside in the criminal justice agency.

Scope

AGENCIES COVERED

Criminal Justice Agencies

The Regulations apply to state and local agencies which have received LEAA funding for the collection, storage, or dissemination of criminal history record information since July 1, 1973. Although the number of agencies covered varies among states, the major metropolitan city and county law enforcement departments and the state law and correction departments are generally affected.

Non-Criminal Justice Agencies

Non-criminal justice public agencies and private companies may also be affected since the Regulations prescribe standards to protect criminal history information from misuse by employees of agencies or organizations authorized to perform services in connection with criminal history information system operation (e.g., where data processing, microfilming, equipment repair, janitorial services or other activities that involve access to criminal history information are performed by non-criminal justice personnel).

The Shared Computer System

Where criminal justice information is maintained in a "shared" computer system operated by a non-criminal justice agency, the requirements of the Regulations apply only to personnel and procedures involved in the criminal history system operations and do not apply to personnel employed in other areas of the computer center.

INFORMATION COVERED

The administrative security requirements of the Regulations apply *only* to systems which include criminal history information which is retrievable by name or other personal identifier of the record subject.

In general terms, the Regulations define "criminal history information" as information containing an individual's name or identifier such as identification number, and notations of arrests or other formal criminal charges, and any subsequent disposition and/or other criminal justice actions relating thereto, including dismissals, decisions to drop charges, and so forth

Since the Regulations do not apply to intelligence, identification, and other non-criminal history information, the administrative security requirements are not applicable to systems containing this type of data. Application, however, of similar procedures would generally be appropriate to the operation of systems maintaining such information.

SCOPE OF THIS GUIDE

This guide, "Administrative Security" is limited to a discussion of those administrative, personnel, and related procedures which can be adopted to protect against unauthorized misuse, disclosure or destruction of criminal history information. For this reason, procedures to ensure physical security and to develop internal computer controls are not discussed here.

Similarly, those administrative procedures whose objective is to ensure data accuracy, completeness, dissemination limits, etc., are not discussed here. Such related concepts are individually covered in each of the other guides as appropriate (e.g., the security requirements involving inspection of records are explained in "Privacy and Security of Criminal History Information: A Guide to Record Review and Challenge").

Procedural Requirements

- GENERAL
- AUTHORIZED ACCESS
- EMPLOYEE SCREENING
- TRAINING/ACCOUNTABILITY
- DISCIPLINE
- THE "SHARED" COMPUTER SYSTEM

GENERAL

Many people have observed that, no matter how sophisticated the system of physical security and technological safeguards which an agency establishes to protect its records, the system will not be secure if the employees do not make a conscious effort to implement security. The Regulations recognize this problem and establish a general framework of security standards that leave the development of specific implementation procedures to individual agencies.

AUTHORIZED ACCESS

To ensure that access to criminal history information is limited to authorized personnel it is necessary that procedures be established for both "position clearance" (e.g., designation of job positions authorized to have various levels of data access) and "employee screening" (e.g., review of specific individuals prior to assignment to job positions having authorized access to data or system facilities).

Since the Regulations allow criminal history systems to operate in either a "shared" or "dedicated" computer environment, some requirements and procedures may vary depending upon this basic distinction, e.g., whether the criminal history system is operated within a criminal justice agency or by a non-criminal justice agency such as a state data processing center.

In the following sections these variations are clearly identified.

The following is a check list of sample "position clearance" procedures:

—Identify all personnel positions having a need to access criminal history information and/or to have access to criminal history system facilities for job performance (see Exhibit I, pg.12).

—Identify types of records for which preaccess position clearance would be appropriate-e.g., in an automated system, clearance would be appropriate for employees with access to printouts (which contain historical information), tapes (on which the data is stored), software programs (which manipulate data), printed records (which describe the software) terminals, computer, etc.

—Assign an appropriate access level to all personnel according to the extent that use of, or access to, criminal history information or system facilities is required for job performance (including personnel requiring access to areas where information is stored but having no need to use or see the data—such as janitors, etc.) (see Exhibit II, pg. 13).

—Develop a formal listing of positions having authorized access to data.

—Establish (or in the case of a shared computer system, approve) procedures to ensure compliance with access limitations (see Exhibit III, pg. 14).

EXHIBIT I

Positions with Potential Access to Criminal History Information

The following is a list of the types of employee positions generally having some level of authorized access to criminal history information and/or system facilities. The list includes *sample positions only* and individual agencies should review their operation to see if other employees are involved.

- Criminal justice agency employees who normally utilize or are required to have access to criminal history records for criminal justice purposes.
- Criminal justice agency employees who work in areas where criminal history records are maintained.
- Employees of other agencies or private companies who work with criminal history records.
- Employees of non-criminal justice agencies or private companies who work where criminal history records are maintained.

A sample of specific jobs coming within these categories are:

- Records clerks.
- Line personnel, e.g., patrol personnel.
- Secretaries.
- Security personnel.
- Microfilmers.
- Custodial personnel.
- Repair personnel.
- Computer personnel.
- Consultants.

EXHIBIT II

Levels of Access

The following is a list of differing levels of access which may be appropriate for different positions.

Manual System

Employee has authority to:

- Enter records area and directly obtain records and remove records for use, distribution, or data entry.
- Enter records area and obtain records from records personnel only.
- Enter records area in order to repair or maintain the record-keeping system.
- Request records but not enter records area.
- Request limited classes of records only.

Automated System

Employee has authority to:

- Operate terminal and obtain records for use, dissemination, or data entry.
- Operate terminal and obtain records for use or distribution (no data entry).
- Operate terminal but not obtain criminal history information.
- Operate or program computer and access, change, or delete records through computer console or control terminal.
- Operate or program computer but *not* access, change, or delete records through computer console or control terminal.
- Enter computer or terminal area and obtain records from terminal operator.
- Enter computer area to repair or maintain terminal.
- Enter computer area for purposes unrelated to record access.
- Request records but not enter terminal area.

EXHIBIT III

Procedures to Implement Access Limits

The following types of procedures can be used to ensure compliance with access limits.

— color-coded badges
— sign-in logs
— computer sign-on codes

Note: Where criminal history data is maintained by a non-criminal justice agency (e.g., in a shared computer environment) the criminal justice agency entering the data should obtain the authority to develop and/or approve the procedures to be used to ensure limitations on authorized access to criminal history information.

EMPLOYEE SCREENING

The Regulations require that a criminal justice agency screen all personnel authorized to have direct access to criminal history information. Although not required by the Regulations, screening procedures should also be applied to individuals who are authorized to work in areas where criminal history information is maintained (see list in Exhibit I).

Where criminal history information is maintained in a "shared" environment and/or handled by non-criminal justice personnel (e.g., a private repair service), the Regulations permit screening to be performed by either the criminal justice agency supplying the data or the non-criminal justice agency employing and assigning the personnel (pursuant to criteria developed or approved by the criminal justice agency).

Criminal Justice Agency Personnel

Criminal justice agencies do not have to screen their own employees separately (e.g., pre-employment screening procedures already in use are acceptable under the Regulations and agencies need only establish a job clearance system to establish levels of authority to access criminal history information as discussed in the preceding section).

Non-Criminal Justice Personnel

It should be noted that the authority to screen non-criminal justice personnel is not the same as the power to determine which individuals will be hired. The power to screen is only the power to reject, based on good cause, an employee for work with criminal history information or in areas where such information is located.

The following is a check list of sample procedures which can be used by a criminal justice agency to comply with the requirements for "screening" of non-criminal justice personnel having authorized access to criminal history information:

— List all public non-criminal justice agencies and private companies which are affected by the Regulations (e.g., whose personnel might have access to criminal history records or system facilities) such as repair personnel.

— Determine the appropriate method of implementation for each agency or company and brief the affected agency or company.
(e.g., The screening system could be enforced through a contract, provisions in civil service regulations, incorporation in the employment policies of the agency or company, local ordinance, state statute, etc.).

— Determine (and agree in writing) whether screening will be conducted by the criminal justice agency directly or by the non-criminal justice agency or organization employing the personnel who will have access to the criminal history information system.

— Determine and where appropriate, agree in writing upon the selection criteria.
(Although the screening is obligatory, the Regulations do not determine the selection criteria. Each criminal justice agency is able to determine what criteria are most suitable for its operational needs and the level of record access which will occur, consistent, however with state law, civil service regulations, etc.)

— Determine (or where screening is to be performed by a non-criminal justice agency, agree in writing to) procedures which will be used to screen specific categories of employee applicants.
  (e.g., Depending on the selection criteria, screening could be accomplished, for example, by a personal interview, or check against agency records, or check against agency, state, or Federal Bureau of Investigation (FBI) records.)

— Develop a notice which explains the purpose behind the screening procedures for distribution when members of the public or affected employees inquire.

— Implement screening procedures.
  (e.g., Advise appropriate administrative offices if screening is to be done within the criminal justice agency or, if screening is to be done by the non-criminal justice agency, ensure that procedures are followed prior to job assignment by the non-criminal justice agency.)

— Prepare (or obtain from the relevant non-criminal justice agency) a list of approved personnel and approved levels of access.

TRAINING/ACCOUNTABILITY

The Regulations require that every employee who works with criminal history information or works in areas where it is located must be made familiar with the substance and intent of the Regulations. The level of training needed to comply with these requirements depends on the degree of interaction which the employee has with the protected information and the record-keeping apparatus; each criminal justice agency may provide the training which it deems appropriate.

The Regulations also require that criminal justice agencies institute procedures which assure that employees who work with criminal history records (see list in Exhibit I) take responsibility for the physical security of information under their control, or within their custody, and protect the information from unauthorized access, disclosure, or dissemination.

For employees who will simply be around criminal history information, and system facilities, posters and department memoranda *may* be adequate forms of training. Where the employees will manipulate, use and in particular, disseminate criminal history information frequently as part of their employment, some kind of institutionalized, or classroom, training program should be implemented with both initial and follow-up training.

Additionally, although not specifically required, it is generally recommended that agency standards and procedures relating to administrative security or other requirements be developed in written form and made directly available to personnel within the agency. Development of simplified brochures or other "easy-to-read" materials may be appropriate for this purpose. Such material should include a statement of possible penalty for violation of such policies, for example, the transfer of personnel, who have violated the procedures, to other duties.

DISCIPLINE

If an employee of a criminal justice agency violates security regulations, the agency may decide to transfer that employee to a less sensitive position, or take other actions as prescribed by the agency's policies. The Regulations require that any employee of a non-criminal justice public agency or private company who works with criminal history records or in areas where they are maintained also be subject to the possibility of transfer. Specifically, they require the criminal justice agency to obtain the right to initiate, or cause to be initiated, administrative action leading to the transfer or removal of personnel who violate these regulations or other security requirements established for the collection, storage, or dissemination of criminal history information.

The authority provided by the Regulations is a limited authority. The criminal justice agency may not insist on the transfer of an errant employee; it may only insist that administrative proceedings occur. The procedures to be followed, the rights of the accused, and the method for determining the results shall be under the control of applicable other appropriate regulations.

THE "SHARED" COMPUTER SYSTEM

Often, when a criminal justice agency automates part or all of its record-keeping system, the computer services are provided by a non-criminal justice public data processing agency and the system is located within that agency's facility. When this occurs, the administrative security regulations require the criminal justice agency to develop or approve and to have authority to audit, monitor and inspect the procedures and features of those aspects of the automated system which involve the criminal history system. This includes: the procedures affecting operation of the tapes or discs on which the information is stored, the software programs which manipulate, process, or protect the information, the printed records which describe the software, the printouts which show criminal history information, the computer and its peripheral equipment, etc.

Basic Requirements

In general terms, the Regulations require that a criminal justice agency must have authority to develop and/or approve procedures which will be followed by the non-criminal justice agency to ensure that:

- Criminal history information will be stored in the computer in a way that it cannot be modified, destroyed, accessed, changed or overlayed in any fashion by a non-criminal justice terminal.
- Software programs will be utilized to prohibit inquiry, record updates, or destruction of records from other than authorized criminal justice terminals.
- Software programs will be utilized to maintain information on all unauthorized attempts to penetrate the system.
- Software programs utilized to prohibit and/or detect unauthorized access are maintained under maximum security and are known only to criminal justice personnel (and other persons designated pursuant to specific agreement).

Additionally, as indicated in previous sections, the criminal justice agency must ensure:

— that access to criminal justice information and facilities will be limited to authorized employees.
— that employees having authorized access to criminal justice information and/or system facilities will be screened (by the data processing or criminal justice agency) pursuant to criteria established or approval by the criminal justice agency and consistent with applicable or other appropriate requirements.
— that non-criminal justice employees authorized to have access to criminal justice data and/or system facilities will be advised of (or trained in) the security provisions of these Regulations (by the criminal justice agency or data processing centers).
— that procedures will be followed to detect unauthorized access to or use of data by non-criminal justice personnel and that authority exists in the criminal justice agency to initiate (or cause to have initiated) administrative proceedings leading to transfer of individuals found to violate applicable security provision.
— that the criminal justice agency will have the authority to audit, monitor and inspect all aspects of administrative security adopted pursuant to the Regulations.

Implementation

The Regulations on administrative security establish a protective framework in which criminal justice agencies must relate to non-criminal justice public agencies and private companies in order to provide for the security of criminal history information.

The Regulations give each criminal justice agency the discretion to determine how it will implement these requirements. The most commonly accepted method of implementation would be a contract which provides the criminal justice agency with assurances that it may exercise the required authority. But, an ordinance, regulation, or statute which gives criminal justice appropriate authority would be sufficient. Voluntary adoption by the non-criminal justice public agency or private company of internal regulations which provide for implementing the administrative security requirements would also be sufficient, provided that the internal procedures were incorporated as part of an overall operating agreement with the criminal justice agency. In either case, although not specifically noted in the Regulation, it is *strongly* recommended that assurances relating to provisions discussed above be included in some type of formal and written document. A sample of such agreement is set out on page 25.

Questions and Answers

Q: Can I prevent, by the screening and rejection process, an applicant for employment at another agency from getting a job?

A: No. But you may prevent him or her from being assigned to work with or in the area of criminal history records.

Q: Can a criminal justice agency employ a private data processing center to process criminal history record information for it?

A: The regulations do not prevent such employment as long as the private center is willing to agree to the constraints contained in the administrative security regulations.

Q: Everything in our record system is, under state law, open to public inspection. Do the administrative security regulations still apply?

A: Yes. Even though the information in your file is open to public inspection, your agency still needs to protect the file from illegal access and possible destruction or mutilation. The administrative security regulations support these objectives.

Q: May special security procedures be utilized for software programmers who will work on protective software for automated systems?

A: Yes. Besides the usual access approval, a criminal justice agency may decide which aspects of protective software a programmer may know about and whether or not the programmer may know such software in its entirety.

Q: Is screening necessary for janitorial personnel who only enter the record area at night when the records are locked up?

A: Yes. Even if the records are locked up, there is still some risk of record mutilation or destruction. Screening criteria would be less stringent, however, than criteria to be applied to employees having greater access.

Q: My records system is maintained at an electronic data processing agency. Do I have to screen janitors and repair personnel from the public work agency who may enter offices in my department?

A: Yes. Employees from other public agencies who will enter offices such as the offices of detectives in a law enforcement agency where copies of criminal history information are likely to be stored or work in the areas of computer terminals which may obtain criminal history information must be subject to some screening prior to assignment to your office. As indicated, standards for such screening might not, however, be the same as standards apply to personnel having direct contact with criminal justice information.

Q: The data processing agency which processes my information claims to be a criminal justice agency. Is this possible?

A: Yes. A data processing agency is a criminal justice agency under the Regulations if it is a government agency or subunit thereof which processes criminal history information pursuant to a statute or executive order and allocated more than one-half its budget to the processing of criminal history information. In the event that the agency meets this test, it has the same authority regarding information protective measures which otherwise would be subject to the approval, inspection audit, and monitoring of the criminal justice agency for whom the system is operated.

Q: What about the situation in many smaller agencies where police records are maintained by a city records clerk?

A: The city clerk's office, even if composed of only one person, must be treated like a separate agency and must agree to the administrative security standards.

Q: Can I employ Comprehensive Employment and Training Act employees if the government will not permit a criminal history record check and they will use criminal history records in my agency?

A: Yes, as long as you follow some kind of screening procedure; the Regulations require screening, but they do not specify the criteria to be applied.

MODEL AGREEMENT OR MEMO OF UNDERSTANDING

In the following, the criminal justice agency is referred to as Agency and the electronic data processing agency is referred to as EDP.

A. Agency Policy Making Authority

1. EDP agrees that destruction of automated records is limited to terminals and terminal users specifically designated by the Agency. It is understood that designated terminals will be under direct Agency control.

2. EDP agrees to undertake subject to Agency approval procedures to insure that CHRI is stored by the computer in such a manner that it cannot be modified, destroyed, accessed, changed, purged, or overlaid in any fashion by non-criminal justice terminals.

3. EDP agrees that Agency may develop or that EDP will develop, subject to Agency approval, programs that:
   a. Prohibit inquiry, record updates or destruction of records from any terminal other than criminal justice terminals which are so designated.
   b. Detect and store records of all unauthorized attempts to penetrate any CHRI system, program, or file.

4. EDP agrees that although various programmers may contribute to the programs described in Section 3, only designated Agency employees and those EDP personnel designated by Agency shall know the programs in their entirety. All EDP programmers who contribute to the programs shall be approved by Agency according to the personnel procedure set forth below.

5. EDP agrees to keep programs described in Section 3 under maximum security conditions.

B. Employment, Accountability, Access Restraint, Training

1. EDP will identify personnel that have authorized access clearance to criminal history information and indicate what level such clearance is for, i.e., access to programs, records, etc., or only to the space where data is maintained, etc.

2. EDP agrees that Agency will screen and have the right to reject for employment, based on good cause, all EDP personnel to be authorized to have direct access to criminal history record information.*

3. EDP agrees that Agency may screen and reject for access, based on good cause, the employees of other agencies and organizations permitted by EDP to enter the computer who may have access to criminal history record information.*

4. EDP agrees that with regard to personnel and employees eligible for screening under Section (1) and (2), Agency may promulgate policies and procedures to insure that these individuals are responsible for the physical security of CHRI under their control or in their custody and the protection of such information from unauthorized access, disclosure, or dissemination.*

5. EDP agrees to initiate, or permit Agency to initiate, administrative action leading to the transfer or removal of EDP personnel eligible for screening under Section (1) where such personnel violate the provisions of these Regulations or other security requirements established for the collection, storage, or dissemination of criminal history record information.

6. Agency agrees that the day-to-day supervision of the personnel and employees eligible for screening under Sections (1) and (2) shall be undertaken by the supervisory staff of EDP.

7. EDP agrees that personnel and employees eligible for screening under Sections (1) and (2) will be made available to Agency for training to insure that they are familiar with the substance and intent of Title 28.

C. Right to Monitor

1. EDP agrees that Agency shall have the authority to audit, monitor, and inspect, all procedures established pursuant to Section A and B.

D. Security Measures (Not included in this publication)

*NOTE: EDP can perform the tasks set aside for Agency pursuant to a written agreement between the two.

☆ U.S. GOVERNMENT PRINTING OFFICE :1978 O—281-380 (4520)

PRIVACY AND SECURITY DOCUMENTS

OTHER PUBLICATIONS IN THE SERIES

Privacy and Security of Criminal History Information: A Guide to Dissemination (NCJ 40000)

Privacy and Security of Criminal History Information: A Guide to Record and Review (NCJ 48125)

Privacy and Security of Criminal History Information: A Guide to Administrative Security (NCJ 49110)

Privacy and Security of Criminal History Information: A Guide to Audit (to be released)

Privacy and Security of Criminal History Information: A Compendium of State Statutes (NCJ 48981)

Privacy and Security of Criminal History Information: An Analysis of Privacy Issues

Privacy and Security of Criminal History Information: A Summary of State Plans

Privacy and Security Planning Instructions (NCJ 34411)

Confidentiality of Research and Statistical Data (NCJ 47049)

Confidentiality of Research and Statistical Data: A Compendium of State Legislation (NCJ 44787)

END