SECTION 1--WHAT IS NCIC 2000?

1.1 DEFINITION

1. The National Crime Information Center (NCIC) 2000 is the System replacing the NCIC System. NCIC 2000 has the same mission and the same basic functionality as NCIC, but also features new capabilities which are described in this operating manual. Just as NCIC, NCIC 2000 is a nationwide, computerized information system established as a service to all criminal justice agencies--local, state, and federal. The goal of NCIC 2000 is to help the criminal justice community perform its duties by providing and maintaining a computerized filing system of accurate and timely documented criminal justice information. For NCIC 2000 purposes, criminal justice information is defined as "information collected by criminal justice agencies that is needed for the performance of their legally authorized, required function. This includes wanted person information; missing person information; unidentified person information; stolen property information; criminal history information; information compiled in the course of investigation of crimes that are known or believed on reasonable grounds to have occurred, including information on identifiable individuals; and information on identifiable individuals compiled in an effort to anticipate, prevent, or monitor possible criminal activity." The NCIC 2000 data bank can best be described as a computerized index of documented criminal justice information concerning crimes and criminals of nationwide interest and a locator file for missing and unidentified persons.

2. The structure and basic procedures of the NCIC System were approved by resolution of the full membership of the International Association of Chiefs of Police in Philadelphia, Pennsylvania, in October 1966 and apply to the new NCIC 2000 System. General policy concerning the philosophy, concept, and operational principles of the System is based upon the recommendations of the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB) to the Director of the FBI. The APB is comprised of top administrators from local, state, and federal criminal justice agencies throughout the United States. Through the APB, its Subcommittee and Working Group input, changes in current applications, the addition of new files, and new procedures, e.g., edits, codes, validations, are coordinated with all NCIC and NCIC 2000 participants.

3. The NCIC 2000 System stores vast amounts of criminal justice information which can be instantly retrieved by and/or furnished to any authorized agency.

4. The NCIC 2000 System serves criminal justice agencies in the 50 states, the District of Columbia, Puerto Rico, and Canada. Through established state systems, the NCIC 2000 System has become available for use by all criminal justice agencies. Access to the NCIC 2000 Vehicle, Boat, Vehicle/Boat Part, and License Plate Files by specific foreign nations is provided through INTERPOL.

1.2 DATA AND PROBABLE CAUSE

1. An NCIC 2000 hit alone is not probable cause to arrest, but indicates that a stolen property report, missing person report, or warrant, etc. may have been filed. A hit is only one element comprising sufficient legal grounds for probable cause to arrest.

2. Correct NCIC 2000 procedure requires the agency which placed the record in file be contacted by the inquiring agency to confirm that the data are accurate and up-to- date. In some circumstances, the hit confirmed with the originating agency may be the major or only element necessary to detain or make an arrest. For instance, a confirmation of an outstanding warrant on an individual or a hit confirmed on a stolen vehicle or stolen property in a timeframe very close to the time of an actual theft would likely support an arrest decision. The confirmation of a hit on a person file record, regardless of how long it had been in the System, would be enough cause to take appropriate action. However, when attempting to recover the stolen property record that had been in the System one or two years, the officer would need not only the element of the hit but also additional facts adding up to probable cause. For instance, a hit on a record two years after a vehicle was stolen would in itself be inadequate probable cause for an arrest, since it would be possible or even probable the vehicle was then in the possession of an innocent purchaser rather than the original thief. To make an arrest under these circumstances, the officer would need not only the element of the hit but also additional facts adding up to probable cause. A hit confirmed with the originating agency can be adequate grounds to recover stolen property, return a missing person, arrest a fugitive, or charge a subject with violation of a protection order.

3. Files, such as the Violent Gang and Terrorist Organization, Convicted Person on Supervised Release, Convicted Sexual Offender Registry, Protection Order, and US Secret Service Protective, do not require hit confirmation and are designed to provide law enforcement officers with adequate warning regarding individuals who have had involvement in criminal activities or are known to represent potential danger to the public.

1.3 RESPONSIBILITY FOR RECORDS

1. NCIC 2000 records must be kept accurate and up-to-date. Agencies that enter records in the NCIC 2000 System are responsible for their accuracy, timeliness, and completeness. To facilitate compliance with hit confirmation requirements, the originating agency must be available 24 hours a day to confirm its record entries. Nonterminal agencies must sign a "Holder of the Record" agreement with a 24-hour agency delineating the responsibility for hit confirmation. Originating agencies that are not available 24 hours must place instructions for after-hour hit confirmation, e.g. a 24-hour contact telephone number or an Originating Agency Identifier (ORI) in the Miscellaneous Field.

2. Stringent administrative procedures and controls to ensure that accurate data are entered in computerized criminal justice information systems are important. An officer's evaluation of the information contained in a hit

response is just as important as keeping the information accurate, timely, and complete. Combining stringent administrative controls with proper evaluation by the officer receiving the hit can prevent lost court cases, civil liability suits, false arrests, and criminal charges against the law enforcement officer.

3. The FBI, as manager of the NCIC 2000 System, helps maintain the integrity of the System through:
   1. Automatic computer edits which reject records with certain common types of errors in data;
   2. Automatic purging of records after they are on file for a prescribed period of time;
   3. Quality control checks by FBI personnel; and,
   4. Distribution of records to be validated. (Details concerning quality control and validation procedures appear in Section 3 of this Introduction.)

4. The NCIC 2000 System makes centralized crime data immediately available to the criminal justice community. The success of the System depends upon the extent to which patrol officers, investigators, judges, prosecutors, corrections officers, and other criminal justice agency officials intelligently use it in day-to-day operations.

5. This manual contains instructions designed to guide participants in using the NCIC 2000 System. No system can be expected to produce results unless it is properly used. The standards and procedures set forth should be strictly followed as every exception tends to degrade the System and the integrity of the data stored in the System.

6. All inquiries regarding the NCIC 2000 System should be addressed to the FBI, CJIS Division, Attention: NCIC 2000, Module E-3, 1000 Custer Hollow Road, Clarksburg, West Virginia 26306-0153.

1.4 SYSTEM DESCRIPTION

1. System participants include local, state, and federal criminal justice agencies throughout the United States, Puerto Rico, and Canada.

2. Most records are placed directly into the NCIC 2000 System by an originating agency (agency holding warrant, missing person report, or theft report; registration information on convicted sexual offender, convicted person on supervised release, etc.), through a control terminal tied into the network. Entries for the Originating Agency Identifier (ORI) File are made by FBI CJIS staff. Records for fugitives wanted by foreign countries are entered either by the Royal Canadian Mounted Police or the U.S. National Central Bureau, INTERPOL. U.S. Secret Service Protective File records are entered by that agency. Records on deported felons are entered by the Immigration and Naturalization Service. Interstate Identification Index (III) records are placed on file by the FBI based on fingerprint cards submitted by the states. The records entered must meet the criteria established for the particular type of record involved. Inquiries must contain prescribed identifying data.

3. NCIC 2000 provides virtually uninterrupted operation 24 hours a day, 7 days a week. Communication lines and associated costs from the NCIC 2000 computer to the control terminals are borne by the FBI.

4. The FBI NCIC 2000 computer equipment can interface with control terminal equipment manufactured by many of the major computer firms. System participants are not required to use the same make computer equipment as that used by the FBI. The only requirement is that terminal equipment be able to communicate with either 8 level ASCII Bisynchronous computer to computer (BiSync), Transmission Control Protocol/Internet Protocol (TCP/IP), or IBM System Network Architecture (SNA) protocol.

1.5 POLICY

1. The CJIS APB recommends general policy to the FBI with respect to the philosophy, concept, and operational principles of the NCIC 2000 System. In its deliberations, the APB places particular emphasis on the continued compatibility of NCIC 2000 and state systems; System security; and rules, regulations, and procedures to maintain the integrity of NCIC 2000 records.

2. The CJIS Advisory Process is composed of two major components, the CJIS APB and the CJIS Working Groups. The APB is responsible for reviewing policy issues and appropriate technical and operational issues related to the programs administered by the FBI CJIS Division and, thereafter, for making appropriate recommendations to the FBI Director. The 32-member CJIS APB is composed of the following:

   1. Twenty criminal justice agency representatives who are selected by the CJIS Working Groups and appointed by the FBI Director. (Twelve are state-level agency representatives, and eight are local-level agency representatives.)

   2. Three individuals who are selected and appointed by the FBI Director and represent the judicial, the prosecutorial, and correctional sector of the criminal justice community.

   3. Eight individuals who represent professional associations including the International Association of Chiefs of Police, National Sheriffs' Association, National District Attorneys' Association, American Probation and Parole Association, Major Cities Chiefs' Association, the Major County Sheriffs' Association, American Society of Crime Laboratory Directors, and one executive level representative from a national professional association representing the courts or court administration.

   4. The Chairman of the CJIS Federal Working Group.

3. A Federal Working Group and four regional Working Groups were established to recommend policy and procedures for the programs administered by the FBI CJIS Division. These Working Groups are also responsible for the review of operational and technical issues related to the operation of or policy for these programs. The Working Groups make appropriate recommendations to the CJIS APB.

4. To gain insight and direction into specific program-related issues, the APB receives input from standing Subcommittees. These are the NCIC, Identification Services, Sanctions, Security and Access, and Uniform Crime Reporting Subcommittees.

1.6 SYSTEM SECURITY

1. There is no federal legal or policy prohibition against dissemination of information contained in NCIC 2000 files. If no state/local law or policy prohibition exists, authorized indirect dissemination of NCIC 2000/III records is discretionary with the Control Terminal Agency (CTA). Such information may be withheld because of criminal justice priorities, budgetary limitations, or other reasons determined by the CTA to be legitimate.

2. An agency participating in the NCIC 2000 System as a CTA must assume responsibility for and enforce System security with regard to all other agencies which it, in turn, services. The responsibilities of NCIC 2000 CTAs are outlined in Section 4 of this Introduction.

3. The FBI uses hardware and software controls to help ensure System security. However, final responsibility for the maintenance of the security and confidentiality of criminal justice information rests with the individual agencies participating in the NCIC 2000 System. Further information regarding System security can be obtained from the CJIS Security Policy.

4. All state and local agencies participating in the NCIC 2000 System III File are required to adhere to the security guidelines as set forth in the publication, *NCIC: Computerized Criminal History Program Background, Concept and Policy*, and in Subparts A and C of the United States Department of Justice Regulations governing the dissemination of criminal records and criminal history information (Regulations) published in the *Federal Register* on May 20, 1975, and August 7, 1976 (Title 28, Code of Federal Regulations, Part 20). Copies of these documents may be obtained from the FBI CJIS Division, 1000 Custer Hollow Road, Clarksburg, West Virginia 26306. Additional guidelines for state III Files appear in the Regulations published in the *Federal Register* on March 19, 1976. Additional security guidelines can be found in the CJIS Security Policy.

5. The data stored in the NCIC 2000 System and the III File are documented criminal justice information and must be protected to ensure correct, legal, and efficient dissemination and use. It is incumbent upon an agency operating an NCIC 2000 terminal to implement the necessary procedures to make that terminal secure from any unauthorized use. Any departure from this responsibility warrants the removal of the offending terminal from further NCIC 2000 participation.

6. Information can be obtained from NCIC 2000 and the III File both directly and indirectly. Direct access is terminal access and dissemination within that terminal agency. Indirect access is nonterminal access outside of an agency with direct access.

7. The individual receiving a request for criminal justice information must ensure that the person requesting the information is authorized to receive

the data. Dissemination of most file data are discretionary with the CTA, whereas NCIC 2000 Convicted Person on Supervised Release, Convicted Sexual Offender Registry, Violent Gang and Terrorist Organization, inactive Protection Order, and III File data are confidential and should be treated accordingly. Unauthorized request or receipt of NCIC 2000 material could result in criminal proceedings brought against the agencies and/or the individuals involved.

1.7 SYSTEM DISCIPLINE

1. To help ensure the proper operation of the NCIC 2000 System, the standards, procedures, formats, and criteria mentioned in this manual must be strictly followed. In this respect, NCIC 2000 CTAs must not only follow the rules set forth but must also ensure that agencies they are servicing do the same.

2. Complete, accurate, and timely records are essential to ensure System integrity. Users also are encouraged to enter records in a timely manner to afford the maximum protection to the law enforcement officer by providing up-to-date information. Although the use of NCIC 2000 is voluntary, delayed entry of records in NCIC 2000 reduces or eliminates the possibility of apprehending wanted persons, locating missing persons, and recovering stolen property.

3. Promptness in modifying, locating, or clearing records in the System will help to keep the System free of outdated information.

4. NCIC 2000 provides information for decisionmaking by investigators, patrol officers, judges, prosecutors, and corrections officials. The information furnished by NCIC 2000 must be evaluated along with other facts known to the officers, investigators, judges, prosecutors, and corrections officials.

5. When an agency receives a positive response from NCIC 2000 and an individual is being detained or a piece of property can be seized, an immediate confirmation with the agency that originated the record in the System is necessary. This confirmation ensures the validity of the hit before an arrest or seizure is made. Likewise, the originating agency has the duty to respond promptly with the necessary confirmation and other pertinent details. (Hit confirmation procedures can be found in Section 3 of this Introduction.)

SECTION 5--NCIC 2000 STANDARDS AND SANCTIONS

5.1 STANDARDS

The use of "effective communications" to help the criminal justice community perform its duties not only means providing access to and obtaining detailed information from pertinent computerized databases, but also includes the amount of time required to access the databases. While an entry, inquiry, or update message may contain specific and detailed information, the message (communication) could be very ineffective if it cannot be transmitted to the data center and a response cannot be received from the data center within a reasonable amount of time. It is not uncommon to hear of a hit occurring minutes after the record was entered. Restrictions have also been placed on the amount of time that a person may be detained while an inquiry is being made to determine whether a record is on file in a database. The rapid transmission of messages is extremely important, and standards were prepared to ensure that messages are transmitted and processed within a reasonable amount of time.

To ensure the integrity of the System, certain policies and standards must be completed, adopted, and followed. Through these policies and standards, a tool of measurement is provided against which the CJIS APB can measure the performance of the component parts of the System as a whole. These policies and standards also must address the specific areas of complaint of the "special" case situations.

5.2 STANDARDS FOR INQUIRY RESPONSE TIME - HOT FILES (NON-III) FOR SINGLE HIT/NO IMAGE RESPONSES

High-Speed Line - Computer Interface

1. Average message response time for an inquiry from the CTA to NCIC 2000 and back to the CTA should not exceed 2 seconds.

2. Average message response time from a CTA to an agency interfaced with the CTA should not exceed 12 seconds after transmission of the inquiry, with 2 of the 12 seconds allocated to the transmission to, processing by, and return of the response from NCIC 2000 as described in standard 1 above.

3. Average message response time for an end-user terminal interfaced with a local/regional system which is interfaced with a CTA should not exceed 22 seconds after the transmission of the inquiry, with 12 of the 22 seconds allocated to the transmission to, processing by, and return of the response from the CTA and NCIC 2000 as described in standards 1 and 2 above.

4. Average response time from any local/regional system or terminal interfaced directly with the NCIC 2000 computer (i.e., NCIC 2000 lines which terminate at an agency that is not a CTA) to an end-user terminal interfaced with the local/regional system shall not exceed 12 seconds, with 2 of the 12 seconds allocated to the transmission to, processing by, and return of the response from NCIC 2000 as described in standard 1.

5. An additional 10-second allowance can be made for additional network interfaces. These interfaces will include servers to local area or wide area networks, intranets, and wireless communication systems (commercial and private). For example, mobile units connected to a wireless communications system and then connected to a metropolitan server which is interfaced with the CTA and then connected to NCIC will be allowed a 32-second total response time from the initial inquiry.
Note: Average time should be based upon a compilation over a 28-day period. Abnormal operating times, such as during the installation of a new computer, should be excluded from the 1-month compilation.

5.3 STANDARDS FOR RESPONSE TIME - III

1. Average message response time for an inquiry from the CTA to NCIC 2000 and back to the CTA should not exceed 5 seconds.

2. Average message response time from a CTA to an agency interfaced with the CTA should not exceed 15 seconds after transmission of the inquiry, with 5 of the 15 seconds allocated to the transmission to, processing by, and return of the response from NCIC 2000 as described in standard 1 above.

3. Average message response time for an end-user terminal interfaced with a local/regional system which is interfaced with a CTA should not exceed 25 seconds after the transmission of the inquiry, with 15 of the 25 seconds allocated to the transmission to, processing by, and return of the response from the CTA and NCIC 2000 as described in standards 1 and 2 above.

4. Average response time from any local regional system or terminal interfaced directly with the NCIC 2000 computer (i.e., NCIC 2000 lines which terminate at an agency that is not a CTA) to an end-user terminal interfaced with the local/regional system shall not exceed 15 seconds, with 5 of the 15 seconds allocated to the transmission to, processing by, and return of the response from NCIC 2000 as described in standard 1 above.

5. An additional 10 second allowance can be made for additional network interfaces. These interfaces will include servers to local area or wide area networks, intranets, and wireless communication systems (commercial and private). For example, mobile units connected to a wireless communications system and then connected to a metropolitan server which is interfaced with the CTA and then connected to NCIC will be allowed a 32 second total response time from the initial inquiry.
Note: Average time should be based upon a compilation over a 28-day period. Abnormal operating times, such as during the installation of a new computer, should be excluded from the one-month compilation.

5.4 STANDARDS FOR RECORD ENTRY BY USER AGENCY

1. Any agency having investigative authority and jurisdiction and having an FBI CJIS- assigned ORI must enter records into NCIC 2000 which meet NCIC 2000 criteria as soon as reasonably possible after the minimum data for entry is available.

2. The CTA shall be responsible for assuring that every agency which has a terminal or access to a terminal by some interagency agreement and has an FBI CJIS-assigned ORI and investigative authority and jurisdiction may enter records into NCIC 2000.

3. Every agency that enters records destined for NCIC 2000 must assure that hit confirmation is available for all records, except III records, 24 hours a day either at that agency or through a written agreement with another agency at its location.

4. Every agency is responsible for the removal of an NCIC 2000 record as soon as it is aware that the record is no longer valid.

5. Average message response time for an entry from the CTA to NCIC 2000 and back to the CTA should not exceed 5 seconds.

6. Average message response time from a CTA to an agency interfaced with the CTA should not exceed 20 seconds after transmission of the entry, with 5 of the 20 seconds allocated to the transmission to, processing by, and return of the response from NCIC 2000 as described in standard 5 above.

7. Average message response time for an end-user terminal interfaced with a local/regional system which is interfaced with a CTA should not exceed 35 seconds after the transmission of the entry, with 20 of the 35 seconds allocated to the transmission to, processing by, and return of the response from the CTA and NCIC 2000 as described in standards 5 and 6 above.

8. Average response time from any local/regional system or terminal interfaced directly with the NCIC 2000 computer (i.e., NCIC 2000 lines which terminate at an agency that is not a CTA) to an end-user terminal interfaced with the local/regional system shall not exceed 20 seconds, with 5 of the 20 seconds allocated to the transmission to, processing by, and return of the response from NCIC 2000 as described in standard 5 above.

5.5 STANDARDS FOR SYSTEM AVAILABILITY

1. The NCIC 2000 System availability goals shall be 100 percent with 99 percent as minimum acceptable performance.

2. The CTA computer availability goals shall be 100 percent with 98 percent, as minimum availability time.

3. The local/regional computer availability goals shall be 100 percent with 96 percent as minimum.

5.6 STANDARD REGARDING EQUIPMENT AND TECHNOLOGY COMPATIBILITY

Equipment and/or technological incompatibility shall not be sufficient justification for any agency to operate outside of the normal CTA configuration.

5.7 STANDARDS FOR SERVICES AVAILABILITY

Those services provided by NCIC 2000 to the CTAs shall be provided by the CTAs to their users with the exception of:

1. Services specifically limited to CTAs by FBI CJIS policy.

2. Services which are restricted to certain users by nature of their governmental and/or criminal justice status, federal laws, and regulations governing access to certain types of NCIC 2000 services.

3. Services which may be contrary to a state law or executive order.
"Users" include those agencies having a direct telecommunications link with a CTA and any regional dispatch center, electronic switcher, satellite computer, or other computer interface, providing a telecommunications link to user agencies, as well as those agencies who have no telecommunications link but access a CTA via another user which has a tele-communications link. Any regional dispatch/communication center shall be required by the CTA to provide the same services to their users as those provided to them by the CTA.

Services include providing users with:

1. The capability of communicating with and receiving responses from all current and future NCIC 2000 files.

2. The capability to enter an NCIC 2000 record into all current and future NCIC 2000 files which:
   1. Meet the NCIC 2000 entry criteria for the file involved;
   2. Contain at least the minimum data required by NCIC 2000 for entry and up to the maximum number of identifiers permitted in the record by NCIC 2000; and
   3. Contain any of the codes or data permitted by NCIC 2000 in each of the fields.

3. Permission to enter a valid record regardless of the existence of any other record(s) already entered in NCIC 2000 by any other agency(s) for the person or property in question.

4. The capability to add information to, delete information from, and/or change information in a field(s) of an existing NCIC 2000 record.

5. The capability to remove a record from file when a record is determined to be invalid, e.g., the warrant which was the basis for an entry is dismissed or when the missing person or property which is the subject of the record is found.

6. The capability to place a locate against another agency's NCIC 2000 record, including records entered by agencies serviced by the same CTA as well as records entered by agencies serviced by another CTA.
The use of the above services by any user agency shall be in accordance with the instructions and procedures contained in the *NCIC 2000 Operating Manual*, the codes contained in the *NCIC 2000 Code Manual*, and new enhancements contained in NCIC 2000 Technical and Operational Updates, CJIS *Information Letter*, or any other official notification from the FBI CJIS Division.

5.8 INTRODUCTION TO NCIC 2000 SANCTIONS

1. Purging of an agency's NCIC 2000 records and discontinuance of System access for an agency are the two ultimate sanctions available to FBI CJIS management for enforcement of System policy and procedure. This presumes prosecution for law violations which would normally be handled at the state level and directed toward an individual rather than toward an agency. References to CTAs throughout this report include other agencies with direct NCIC 2000 lines when the inclusion is logical.

2. Considerations

1. An up-to-date FBI CJIS/CTA User Agreement should be on file with the FBI CJIS Division, Programs Support Section, and the respective CTA. It should include reference to the sanctions that could be imposed for failure to comply.

2. Specific references should include but are not limited to:
Failure to react properly to error notices
Failure to react properly to hit confirmation requests
Failure to locate
Failure to complete entries/modifications/removals promptly
Failure to make complete entries
Failure to validate
Failure to assure security of equipment and data
Failure to provide qualified operators
Entry of invalid or nonqualified records

3. A special audit of a CTA should be part of the sanction package.

4. Flagging records of substandard CTA lines should be an option.

5. Deadlines should be imposed on compliance with corrective action notices.

6. Letter to CTAs, rather than being titled "Caution," should be drafted in the framework of a "Request to Comply" with NCIC 2000 Standards. When prolonged failure to comply would result in discontinuance of service, the letter should be explicit in announcing the "Probationary Status" of the CTA or in announcing the date probationary status will begin if compliance is not forthcoming before then.

7. Unless the serious nature of a problem requires immediate discontinuance of service, a letter to the state's governor should precede discontinuance of service.

5.9 SANCTIONS

1. An NLETS message transmitted by FBI CJIS to the CTA for all nonserious errors and subsequent redirection of the NLETS message by CTA to offending terminal agency. The CTA is to maintain copy of these messages for follow-up.

2. Verbal notice from CTA to terminal agency for nonserious error intercepted by CTA or intrastate message to offending terminal agencies for nonserious errors or reports thereof. (Note: A record of verbal notices should be retained by CTA for 6 months.)

3. Letter of request for compliance
  1. FBI CJIS to CTO/FSC regarding:

    1. Untimeliness
    2. Inaccuracy
    3. Incompleteness
    4. Unsatisfactory record quality
    5. Unsatisfactory validation
    6. Misuse of system notice of probationary status resulting from audit (30 days to correct deficiencies)
    7. Serious error failure of a CTA to ensure compliance with hit confirmation policy

  2.. CTA to terminal agency

    1. Untimeliness
    2. Inaccuracy
    3. Incompleteness
    4. Unsatisfactory record quality
    5. Unsatisfactory validation
    6. Misuse of System
    7. Notice of probationary status resulting from audit (30 days to correct deficiencies)
    8. Serious error
    9. Failure of the terminal agency to comply with hit confirmation policy
    4. Letter of intent to remove from System if deficiency not corrected
  1. CJIS APB to CTA head

    1. Continuous serious error trend
    2. Audit failure status (not corrected within 30 days of first letter of request)
    3. Intentional misuse of Purpose Codes in III
    4. Continuous failure of CTA to ensure compliance with hit confirmation policy

  2. CTA to terminal agency

    1. Continuous serious error trend
    2. Audit failure status (not corrected within 30 days of first letter of request)
    3. Misuse of III
    4. Continuous failure of the terminal agency to comply with hit confirmation policy

5. Advisory letter to state governor

1. FBI CJIS to governor with copy to CTA

1. Serious error trend
2. Audit failure (30 days to correct)
3. Probationary status has been modified to failure status (additional 30 days to correct)
4. Unsatisfactory record quality trend
5. Report unsatisfactory validation or failure to correct validation

2. CTA to terminal agency - removal of records and discontinuance of service is imminent

1. Serious error trend
2. Audit failure (30 days to correct)
3. Probation status to failure status
4. Unsatisfactory record quality trend
5. Report unsatisfactory validation or failure to correct validation

6. Removal from System includes purge of all records and discontinuance of service pending reinstatement.

1. CJIS APB and FBI CJIS jointly initiate removal of CTA from active System use.
2. CTA may discontinue service to an offending agency and purge that agency's records from state and NCIC 2000 files.

7. Reinstatement

1. Upon satisfactory proof that the offending CTA has corrected its deficiencies, the APB may reinstate.
2. Upon satisfactory proof that the offending agency under review has corrected its deficiencies, the CTA may reinstate. The CTA also has the option to defer to another agency which will then become the new CTA.

SECTION 1--SECURITY AND CONFIDENTIALITY

SECURITY AND CONFIDENTIALITY OF CRIMINAL HISTORY RECORD INFORMATION OBTAINED VIA THE III

Authorization to obtain records via the Interstate Identification Index (III) is governed by federal laws and state statutes approved by the U.S. Attorney General which are applicable to the U.S. Department of Justice, Federal Bureau of Investigation, and the National Crime Information Center (NCIC 2000).

Operators shall use the terminal only for those purposes which are authorized.

Copies of III data obtained from terminal devices must be afforded security to prevent any unauthorized access to or use of the data.

III records shall be maintained in a secure records environment. Such storage of records may be for extended periods only when the III records are key elements for the integrity/utility of the case files/criminal record files in which they are retained.

When retention of III records is no longer required, final destruction shall be accomplished in a secure manner so as to preclude unauthorized access/use. III records should be properly destroyed when the record is no longer current. Because additions or deletions may be made at any time, a new copy should be requested when needed for subsequent use.

The III shall not be used to access a record to be reviewed and/or challenged by the subject of the record. Record requests for this purpose must be submitted in writing either to the FBI Criminal Justice Information Services (CJIS) Division or to the state of record.

The Control Terminal Agency (CTA) shall ensure that all III transactions (both Criminal History Inquiry [QH] and Criminal Record Request [QR]) originating from terminal devices that access the III through the state system shall be maintained on an automated log. This log shall be maintained for a minimum of one year. This automated log shall, in some way, identify the individual initiating each III transaction, as well as the agency authorizing the transaction. III logs shall also, in some way, identify the record recipient. This information can be captured at log-on and can be a name, badge number, serial number, or other unique identifier.

NCIC 2000

VIOLENT GANG AND TERRORIST ORGANIZATION FILE (VGTOF)

OVERVIEW

The NCIC 2000 Violent Gang and Terrorist Organization File (VGTOF) has been designed to provide identifying information about violent criminal gangs and terrorist organizations and members of those gangs and organizations to law enforcement personnel. This information serves to warn law enforcement officers of the potential danger posed by violent individuals and to promote the exchange of information about these organizations and members to facilitate criminal investigations.

Because VGTOF information is based, in part, on investigative information not previously subject to independent judicial review, strict adherence to policy on the security, use, and dissemination of VGTOF information is necessary.

SECURITY

VGTOF information is exclusively for the use of criminal justice agencies for criminal justice purposes. In no case should VGTOF information be disseminated to any noncriminal justice agency.

The security measures to be accorded criminal history record information as set out in the NCIC Security Policy should be followed with respect to the VGTOF and the information contained therein.