TITLE: CONTROL OF CRIMINAL JUSTICE SYSTEM INFORMATION DATA

CODIFIED:	**62.1**
EFFECTIVE:	**07/23/04**
RESCINDS/AMENDS	**NEW DIRECTIVE**
PAGES:	**4**

PURPOSE

The purpose of this directive is to establish procedures and provide direction in the proper use of The New Mexico Law Enforcement Telecommunications System (NMLETS)

DISCUSSION

The New Mexico Law Enforcement Telecommunications System (NMLETS) is a statewide storage and forward message switching system. It was established as a service to all criminal justice and law enforcement agencies within New Mexico. The System operates by means of a computer telecontroller, or switchers, terminal devices and most important operators. Its objective is to improve the effectiveness of law enforcement through the more efficient handling and exchange of documented criminal justice information.

Control and enforcement of all NCIC/NMCIC/NLETS/NMLETS rules and regulations are vested in the New Mexico Department of Public Safety (DPS) Headquarters. The success of the System is dependent on strict compliance by all users. Professional procedures demand all system users conform at all times with established rules and regulations. The computer switcher is located at DPS Headquarters in Santa Fe. The NMLETS computer switcher allows access to the following databases and networks:

A. National Crime Information Center (NCIC) – Located in Washington, DC, and managed by the FBI. NCIC contains sixteen (16) files for inquiry and/or entry of wanted and missing persons and stolen property.

B. National Law Enforcement Telecommunications System (NLETS) – Headquartered in Phoenix, AZ, a network providing access and communications to other states for administrative messages, vehicle registration information, driver's license information, help files, etc.

C. New Mexico Crime Information Center (NMCIC) – Headquartered in Santa Fe, the State database allowing access and entry for wanted person files.

D. New Mexico Motor Vehicle Division (DMV) – Located in Santa Fe, the database allowing access to New Mexico vehicle registration files and driver's license files.

POLICY

It is the policy of the Santa Fe City Police Department to participate in a computerized nationwide and statewide criminal information system. All police personnel having access to the New Mexico Law Enforcement Telecommunications System (NMLETS), National Law Enforcement Telecommunications System (NLETS), National Crime Information Center (NCIC), Interstate Identification Index (III), New Mexico Crime Information Center (NMCIC) and Department of Motor Vehicle (DMV) will adhere to all rules and regulations that pertain to the proper use of these systems.

PROCEDURE

SYSTEM SECURITY

62.1.01 The data retrieved from NMLETS is documented criminal justice information, which must be protected to ensure correct, legal and efficient dissemination and use. It is incumbent upon a terminal agency operating an NMLETS terminal to implement the necessary procedures and actions to make that terminal secure from any unauthorized use. Any departure from this responsibility warrants the removal of the offending terminal from the NMLETS Network. The individual receiving a request for

criminal justice data must ensure that the person requesting the information is authorized to receive the data. The data stored in NMLETS is confidential and should be treated accordingly; any unauthorized request or receipt of NMLETS material could result in criminal proceedings.

62.1.02 The New Mexico DPS, serving as Control Terminal Agency (CTA), will be responsible for service and the enforcement of system security with regard to all NMLETS users.

62.1.03 All terminals must be located in such locations within each agency that they are secure for use and from view of unauthorized persons. State level audits will check each agency's terminal security on a regular basis.

SYSTEM DISCIPLINE

62.1.04 To assure the proper operations of NMLETS, all standard, procedures, formats and criteria stated in the NCIC Operating Manual, NCIC Code Manual, NLETS Operational Manual and NMLETS Operating Manual must be strictly adhered to. Each agency alone is responsible for the accuracy, format completeness and correct status of any message type originated by that agency.

62.1.05 Each terminal agency will be issued a NMLETS Operational Manual, NLETS Operational Manual, NCIC Operational Manual and an NCIC Code Manual. These manuals must be readily available to the operator(s) and all revisions must be posted in the manuals as they are received. Failure to keep current manual at each terminal location may be cause for suspension from the System. All terminal operators will be expected to review all NMLETS/NLETS/NCIC newsletters and NCIC Technical and Operational Updates, which must be made, part of the manuals and incorporated into the use of the System.

62.1.06 All manuals must be kept in a good state of repair. When the binders and/or it contents become damaged or worn, they should be repaired or replaced as soon as possible. The Terminal Agency Coordinator (TAC) should contact the state CTO for replacement of unserviceable manuals.

NONTERMINAL USER AGREEMENTS

62.1.07 Are used to make inquires **ONLY** into NMLETS for a nonterminal agency that has its ORI assigned to another terminal agency, but because of extenuating circumstances, the responsible agency is not used. An example of this situation would be the New Mexico Department of Game and Fish. Their own ORI is assigned to their main terminal in Santa Fe; however, there are Game and Fish officers that are stationed throughout the state. Usually, the officer will utilize a local terminal agency located within his/her district for NMLETS access. The ORI of the terminal agency is used for all transactions and the name/unit number of the requesting officer noted in the control field.

62.1.08 Are Used to perform all transactions, including record entries into NMLETS for a nonterminal agency. The ORI of the terminal agency is used if the ORI of the nonterminal agency has not been assigned to responsible agency, or the nonterminal agency is authorized access to criminal justice information, but does not have an assigned OI. An example of this situation would be a criminal justice agency, such as a municipal court, which is authorized access, but does not have an ORI number.

62.1.09 Are used by a terminal agency that does not have 24-hour capability, but has their traffic routed to a full 24-hour terminal (this is known as alternate routing). The ORI of the non 24-hour terminal is used by the responsible terminal for all transactions. In addition, the non 24-hour agency is required to furnish a copy of ALL records entered into NCIC/NMCIC to the alternate routed terminal for record confirmation purposes.

62.1.10 The original of all agreements must be sent to the state CTO for the final review and approval. The original will then be placed in the terminal agency's master filed maintained at DPS. Both the terminal agency and nonterminal agency are responsible for maintaining up-to-date copies of these agreements at their respective terminal sites.

MANAGEMENT CONTROL AGREEMENTS

62.1.11 Many county and municipal government entities choose to combine their telecommunications

responsibilities in the interest of cost saving measures. Regional or local government organizations established pursuant to statute or ordinance, which collect and process criminal justice information, must have a governing board composed of a majority of criminal justice representatives.

APPROVAL OF MANAGEMENT CONTROL AGREEMENTS

62.1.12 Management control agreements must be submitted to the DPS/CTO for review and approval. The agreement will then be forwarded to FBI/NCIC Headquarters for final approval. Failure to submit management control agreements to the DPS, or operating without properly constituted management control board will be considered grounds for immediate removal from the NMLETS Network.

AGENCY RESPONSIBILITIES

62.1.13 Each NMLETS terminal agency is responsible for terminal equipment, security, accuracy and completeness of its records and maintaining all required by documentation (manuals, records, and logs) as prescribed by NCIC/NMCIC/NLETS/NMLETS and the New Mexico Department of Public Safety. The integrity of the records entered into NCIC/NMCIC is the sole responsibility of the terminal agency.

APPOINTMENT OF A TERMINAL AGENCY COORDINATOR (TAC)

62.1.14 The 1984 NCIC Advisory Policy Board (APB) mandated that each Control Terminal Officer (CTO) ensure that each terminal agency administrator designate an individual to serve as a Terminal Agency Coordinator, who shall assume the responsibility for ensuring compliance with State and NCIC policy and regulations. The TAC must be designated prior to the terminal being activated on-line on the NMLETS Network. The TAC should be an individual who is knowledgeable about telecommunications and the operation of the terminal equipment. When the TAC terminates employment with the terminal agency or is reassigned, a new TAC shall be appointed within ten (10) days. The state CTO will then be notified, in writing, of this new appointment. A new terminal User Agreement must then be executed.

INTERSTATE IDENTIFICATION INDEX (III)

62.1.15 The III is an automated system which facilitates the interstate exchange of on-line Criminal History Record Information (CHRI) between criminal justice agencies. It consists of an index containing individuals' names, aliases, physical descriptors, identifying numbers, fingerprint classifications, and names of the agencies maintaining the criminal history information. It is accessed via (NCIC) by insertion of name and other personal descriptors. There are currently 41 states participating in the III system, with approximately 33 million records available.

AUTHORIZED ACCESS TO III

62.1.16 The United States Department of Justice and federal courts have interpreted Title 28, United States Code (USC), Section 534 (the basic and fundamental authorization for the collection, acquisition, exchange and dissemination of CHRI) to require restricted access to FBI CHRI to criminal justice agencies for criminal justice purposes and to federal agencies authorized to receive it pursuant to federal statute or executive order.

USE OF INTERSTATE IDENTIFICATION INDEX

62.1.17 The use of III is strictly controlled by FBI NCIC and the state is required to enforce III policies and procedures. The Privacy Act of 1974 and the computer Fraud and abuse Act of 1986 are two federal statutes affording criminal and civil liability for violations of privacy and security provisions calling for the cancellation of access rights by criminal justice if the dissemination of CHRI is made outside the receiving department or related agency. Each agency administrator is responsible for the proper use of III by his/her officers and employees. Most states (if not all) also have laws, which criminalize or provide civil liability for misuse/unauthorized dissemination of CHRI. Sanctions for misuse of III are taken against the agency, which can include denial of access to III for flagrant or continued misuse or abuse. The TAC) is

responsible for documenting any violations of III, Insuring that the violation is not repeated to the limit of their authority, and reporting the violation(s) to the agency administrator and the State Control Terminal Officer.

62.1.18 Each and every transaction must be logged on the state furnished III Log. Each column must be completed, including the OCA/Reason column. This column should contain either the case number or warrant number concerning the subject that is being run in III. In the absence of a case or warrant number, a valid reason for the III request must be given, i.e. criminal investigation, narcotics investigation, police employee applicant background investigation, search warrant, etc. All III logs are checked during state and FBI NCIC audits.

62.1.19 NCIC Technical and Operational Update 98-4 states: ***" Any electronic device that uses wireless or radio technology to transmit data may be used for transmission of criminal history record information when an officer determines there is an immediate need for this information to further an investigation or there is a situation affecting the safety of an officer or the general public".*** An officer may request an III over the radio during a traffic stop or other routine stop when the actions of the violator or the circumstances surrounding the initial contact with the violator may warrant a request for III. Once the request has been made, the officer must indicate the purpose of the request and what type of information is being sought, i.e. arrest for narcotics violation, arrest for assault on police officers, escape, etc. Only specific arrests or information that would further the officer's investigation can be given over the radio.

62.1.20 Agency administrators, through their respective TAC, need to ensure that sworn and civilian personnel follow the proper procedures for use and requirements surrounding a request for III. Personnel will NOT use III as a "fishing expedition" or to satisfy his/her curiosity. III is a name check only. The only way to way to positively identify a person or make sure the person being inquired on is the same person of interest is to submit a set of fingerprints to the state crime lab and FBI. A large number of criminal history records for persons born prior to 1956 are not in the automated files, which would return a "no criminal record response". Therefore, an officer should rely on his/her training, common sense and personal safety when dealing with a violator or suspect, not on III.

CRIMINAL JUSTICE AGENCY DEFINED

62.1.21 Criminal justice agency means: (1) Courts; (2) a government agency or any subunit thereof which performs the administration of criminal justice pursuant to a statute or executive order, and which allocates a substantial part of its annual budget to the administration of criminal justice.

ADMINISTRATION OF CRIMINAL JUSTICE DEFINED

62.1.22 The administration of criminal justice means performance of any of the following activities: Detention, apprehension, detection, pretrial release, post-trial release, prosecution, adjudication, correctional supervision, or rehabilitation of criminal offenders.

MANAGEMENT CONTROL DEFINED

62.1.23 Management control is defined as the authority to set and enforce: (1) priorities; (2) standards for the selection, supervision and termination of personnel; (3) policy governing the operation of computers, circuits and telecommunications terminals used to process criminal history record data insofar as the equipment is used to process, store, or transmit criminal history record data.

DRAFTED (awm) 07/03

APPROVED: _____
BEVERLY K. LENNEN
Chief of Police

DATE: 07-23-04