NEW MEXICO
LAW ENFORCEMENT TELECOMMUNICATIONS SYSTEM
AND
THE NATIONAL CRIME INFORMATION CENTER

USER AGREEMENT

BETWEEN THE

NEW MEXICO DEPARTMENT OF PUBLIC SAFETY

AND

____

This agreement is made and entered into this _____ day of ______20__ by and between the Department of Public Safety (hereinafter referred to as *DPS*), and the ______________________ a criminal justice and/or law enforcement agency (hereinafter referred to as *USER AGENCY*). The *DPS* serves as the FBI's CJIS Systems Agency (CSA) in New Mexico for the National Crime Information Center (NCIC), the parent agency for the New Mexico Law Enforcement Telecommunications System (NMLETS) and the New Mexico Criminal Justice Information System (NMCJIS).

Whereas, *DPS* serves as the state agency responsible for the management and operation of the NMLETS, NCIC, and NMCJIS, the purpose of this agreement is to govern the exchange of information between the *DPS* Systems and the *USER AGENCY*. The *DPS* will facilitate local law enforcement and other criminal justice agencies' requests to participate in the information services provided on the *DPS* network, provided the *USER AGENCY* abides by applicable federal and state laws, regulations, policies, and procedures related to these systems.

The *DPS* reserves the right to immediately suspend any *USER AGENCY* furnishing information covered by the terms of this agreement if any terms of this agreement or documents incorporated herein are violated. The *DPS* shall resume furnishing such information upon receipt of satisfactory proof that such violations have been fully corrected or eliminated upon completion of an audit by the designated *DPS* staff.

USER AGENCY will ensure that all personnel having access to all information available through NMLETS and/or NMCJIS will be screened according to the personnel background screening policy prescribed in the FBI CJIS Security Policy. In addition, NCIC Criminal History (III), NCIC and NMCIC wants and warrants checks will be conducted prior to employment. State and National fingerprint-based record checks must be conducted within thirty (30) days upon initial employment or assignment for all personnel, including appropriate IT personnel, having access to the FBI CJIS, NMLETS or NMCJIS systems. *USER AGENCY* will also screen employees having access to record storage areas containing FBI Criminal History (III) data, which includes but is not limited to custodial, support, and/or contractor personnel. If a record of any kind is found, access will not be granted until the CJIS Systems Officer (CSO), or his/her designee can review the matter to decide if access/employment is appropriate. If a felony conviction of any kind is found, access will not be granted.

SECTION 1: NMLETS

THIS SECTION APPLIES TO ONLY NMLETS TERMINAL AGENCIES. IF YOUR AGENCY IS NOT A NMLETS PARTICIPANT PROCEED TO SECTION 2.

1.1 DUTIES OF THE *DPS*: Upon receipt of inquiries from *USER AGENCY* which contain all the data elements required by the NMLETS and NCIC Systems, the *DPS* agrees to furnish the *USER AGENCY* such criminal justice information as is available through the NMLETS and further agrees to furnish record information as is available and authorized from the FBI/NCIC System. The *DPS* agrees to incorporate the necessary rules and regulations of the State of New Mexico, the Federal Government, NCIC, NLETS and NMLETS Operating Manuals into training and to provide specialized training on such rules and regulations to the *USER AGENCY* Terminal Agency Coordinator as well as provide training on at least an annual basis. The *DPS* further agrees to provide NMLETS operational and Hit Confirmation support to the *USER AGENCY*. The *DPS* will maintain an automated log of all hot file and III transactions as prescribed in the FBI CJIS Security Policy.

1.2 DUTIES OF THE *USER AGENCY*: *USER AGENCY* will collect, receive, store, use and disseminate all information covered by the terms of this agreement in strict compliance with all present and future Federal and State laws and regulations, and with all rules, procedures, and policies adopted by the *DPS* as described in the NCIC, NLETS, NMLETS Operating Manuals and the FBI CJIS Security Policy.

1.3 EXECUTORY CLAUSE: It is understood by and between the parties hereto, that the *DPS* is obligated to provide services described in Section 1.1 above to *USER AGENCY* only to the extent that public funds are made available to the *DPS* for that purpose.

1.4 TERMINAL AGENCY COORDINATOR: *USER AGENCY* will designate an individual to serve as the Terminal Agency Coordinator (TAC) who shall be responsible for ensuring compliance with NMLETS and NCIC policy and regulations, including all duties outlined in the NCIC TAC Handbook. The TAC will work directly with the New Mexico CJIS Systems Officer (CSO) or designee on all matters dealing with NMLETS.

1.5 TRAINING OF PERSONNEL: *USER AGENCY* personnel operating NMLETS terminals, including Mobile Data Terminals (MDTs/MDCs), are required to satisfactorily complete the prescribed training as provided by or approved by the *DPS*. The *USER AGENCY* Terminal Agency Coordinator is responsible for ensuring initial training, functional testing, and affirming the proficiency of terminal operators within six (6) months of employment or assignment; biennially, provide in-service retraining, functional retesting, and reaffirmation of the proficiency of terminal operators in order to ensure compliance with NCIC and NMLETS policies and regulations; provide or present entry level training on the use of NMLETS, focusing on the Interstate Identification Index (III) requirements and record quality for criminal justice agency records personnel.

1.6 AUDITS: *USER AGENCY* will allow terminal access to State and Federal Auditors to conduct audits of the agency as prescribed in the NCIC and NMLETS Operating Manuals and the FBI CJIS Security Policy.

1.7 HOURS OF OPERATION: All *USER AGENCIES* with file entry capabilities on NMLETS are required to maintain 24-hour, 7-day-a-week operation. Non 24- hour *USER AGENCIES* are required to enter into an agreement with a twenty-four by seven *USER AGENCY* to act as its alternate terminal as prescribed in the NMLETS Operating Manual.

1.8 HIT CONFIRMATION: *USER AGENCY* shall ensure that the Hit Confirmation procedures as prescribed in the NCIC, NLETS, and NMLETS Operating Manuals will be adhered to.

1.9 QUALITY CONTROL: The Agency Administrator (Agency Designated Administrator) and/or the appointed Terminal Agency Coordinator (TAC) accept responsibility for the timely entry and the validity of all records entered by the *USER AGENCY*. The individual selected as the Terminal Agency Coordinator for your Agency must be identified on the final page of this document (refer to page 12), further noting that any changes to this designation must be communicated within five (5) working days to the NCIC Coordinator for the DPS, at 4491 Cerrillos Road, Santa Fe, New Mexico 87507 or by calling 505.827.9181 or 505.827.3413. Procedures for timely entry and the validation process are outlined in the NCIC and NMLETS Operating Manuals. Measures for purging or canceling entries will be adhered to in order to maintain system integrity. The *USER AGENCY* must fully comply with quality control and Hit Confirmation procedures or risk removal of records from NCIC/NMCIC and possible loss of connectivity to NMLETS.

1.10 DATA DISSEMINATION: The *USER AGENCY* shall record all disseminations of Criminal History Record Information received via NMLETS on the prescribed log. The log shall be maintained and retained for at least one year from the date of transaction. Criminal history requests through the Interstate Identification Index (III) must be in accordance with current III policies and procedures. The *USER AGENCY* must ensure that criminal history information received will only be used for those purposes for which it was provided. In addition all data retrieved from NMLETS will adhere to dissemination regulation outlined in the NMLETS Operating Manual.

1.11 SECURITY: *USER AGENCY* agrees to limit access to information furnished by NMLETS to its own employees and other criminal justice/law enforcement agencies who have entered into this agreement with the *DPS* and/or the *USER AGENCY* to protect the security and privacy of this information.

SECTION 2: NMCJIS

THIS SECTION APPLIES TO ONLY NMCJIS AGENCIES. IF YOUR AGENCY IS NOT A NMCJIS PARTICIPANT PROCEED TO SECTION 3.

2.1 DUTIES OF THE *DPS*: Upon receipt of inquiries from *USER AGENCY* which contain all the data elements required by the NMCJIS, the *DPS* agrees to furnish the *USER AGENCY* such criminal justice information as is available through the NMCJIS and further agrees to furnish record information as is available and authorized from the NMCJIS. The *DPS* further agrees to incorporate the necessary rules and regulations of the State of New Mexico and Criminal Information Sharing Alliance (CISA) to provide specialized training on such rules and regulations to the *USER AGENCY* NMCJIS Agency Coordinator as well as provide training on at least an annual basis.

2.2 DUTIES OF THE *USER AGENCY*: *USER AGENCY* will collect, receive, store, use and disseminate all information covered by the terms of this agreement in strict compliance with all present and future Federal and State laws and regulations, and with all rules, procedures, and policies adopted by the *DPS.* The NMCJIS Agency Coordinator will ensure that a NMCJIS Access Authorization form is submitted to the *DPS* for all personnel utilizing the NMCJIS application. Personnel requiring INTEL level access will submit a completed NMCJIS INTEL Access Request Form to the *DPS* for approval.

2.3 EXECUTORY CLAUSE: It is understood by and between the parties hereto, that the *DPS* is obligated to provide services described in Section 2.1 above to the *USER AGENCY* only to the extent that public and/or CISA funds are made available to the *DPS* for that purpose.

2.4 TRAINING OF PERSONNEL: *USER AGENCY* personnel operating New Mexico Criminal Justice Information System (NMCJIS) workstations are expected to satisfactorily complete the initial training as provided by or approved by the *DPS*. The *USER AGENCY* NMCJIS Agency Coordinator is responsible for ensuring initial training. Personnel requesting INTEL level access must complete 28 CFR Part 23 Training prior to INTEL access being granted.

2.5 NMCJIS AGENCY COORDINATOR: *USER AGENCY* will designate an individual to serve as the NMCJIS Agency Coordinator who shall be responsible for ensuring compliance with NMCJIS and CISA policy and regulations.

2.6 QUALITY CONTROL: The agency administrator and/or the appointed NMCJIS Agency Coordinator accept responsibility for the validity of all records entered by the *USER AGENCY*. Measures for entering and updating NMCJIS data will be adhered to in order to maintain system integrity. The individual selected as the NMCJIS Agency Coordinator for the *USER AGENCY* must be identified on the final page of this document (refer to page 12), further noting that any changes to this designation shall be communicated within five (5) working days to the NCIC Coordinator for the DPS, P O Box 1618, 4491 Cerrillos Road, Santa Fe, New Mexico 87507 or by calling 505.827.9181 or 505.827.3413. The *USER AGENCY* shall fully comply with quality control procedures or risk possible loss of workstation connection to NMCJIS.

2.7 DATA DISSEMINATION: The *USER AGENCY* shall ensure that retrieval and dissemination of NMCJIS data is in accordance with the disclaimer clauses presented in the NMCJIS application.

2.8 SECURITY: *USER AGENCY* agrees to limit access to information furnished by NMCJIS to its own employees and other criminal justice/law enforcement agencies who have entered into this agreement with the *DPS* and/or the *USER AGENCY* to protect the security and privacy of this information.

SECTION 3: TECHNICAL AND SECURITY

THIS SECTION APPLIES TO ALL AGENCIES THAT UTILIZE THE *DPS* NETWORK.

3.1 DUTIES OF THE *DPS*: The *DPS* will provide 7 day-a-week, Technical Support specialists via the *DPS* Help Desk. The *DPS* will provide after hours technical support via on-call personnel. Through these mechanisms the *DPS* will provide support to:

1. Verify that the connectivity to the *DPS* network is operational.
2. The *DPS* will be responsible for providing application software to the *USER AGENCY* that supports the intent of this agreement and connectivity to the DPS.
3. Answer and troubleshoot questions and problems directly associated with the applications the *DPS* provides. These applications include, but may not be limited to, NMLETS and CJIS.
4. Work with the *USER AGENCY* to design and implement internetworking solutions that are both secure and mutually beneficial to each agency's processes. Work with the *USER AGENCY* to provide knowledge transfer for the implemented technologies.
5. Storing and creating audit logs with information about events that occurred on the firewall, host system, or network.
6. Notifying *USER AGENCY* of update schedules, system requirements, recommended standards, etc.

The *DPS* will not be responsible for:

1. Non-DPS supported software and/or applications.
2. Hardware components such as, PC's, printers, switches, routers, wiring, etc.
3. PC Operating Systems.
4. Initial and on-going maintenance (patches, updates, etc) on any and all of the above.

3.2 DUTIES OF THE *USER AGENCY*: *USER AGENCY*, by affixing the appropriate signature to this document, hereby agrees that the *USER AGENCY* is responsible for all initial, recurring and replacement costs and support associated with connectivity to the *DPS* network; this includes but is not limited to PCs, routers, circuits, printers, etc. Further, the *USER AGENCY,* by affixing the appropriate signature to this document, hereby agrees that the *USER AGENCY* is responsible for all initial, recurring and replacement costs and support associated with additional security measures recommended by the *DPS* which are required in the FBI CJIS Security Policy.

The *USER AGENCY* understands, agrees and accepts that the *USER AGENCY* is responsible for all PC support which includes loading and set up of the *DPS* application software as provided. The *USER AGENCY* will notify the *DPS* at least five (5) business days prior to adding and/or replacing any existing workstations with access to NMLETS and/or NMCJIS. The *USER AGENCY* is responsible for implementing and maintaining virus protection software on local network devices. The *USER AGENCY* hardware and software must meet the minimum specifications published by the *DPS* by **February 28, 2005** or the *USER AGENCY* shall be removed from the network. The *USER AGENCY* devices that are connected to the *DPS* network shall be named according to the *DPS* authorized/approved naming convention.

The *USER AGENCY* shall request in writing to the *DPS* ITP personnel and receive written approval for any new, as well as any modifications to existing, connections or circuits prior to the *USER AGENCY* entering into any contracts or ordering such circuits from a vendor. Any *USER AGENCY* with connectivity to another organization's network and/or the Internet shall implement the security technologies outlined in the NMLETS Operating Manual. Along with the implementation of the aforementioned security technologies, the *USER AGENCY* must provide the *DPS* with or cooperate with *DPS* personnel to create documentation of these external links. All internetworking solutions to be implemented on networks with connectivity to the *DPS* must also be submitted in writing and receive written approval prior to the *USER AGENCY* entering into any contracts or supplying funds for such solutions. All submissions referenced in this paragraph are subject to approval by the *DPS* ITP personnel to ensure compliance with security regulations.

3.3 TECHNICAL AUDITS: *USER AGENCY* will allow terminal access to State and Federal Auditors to conduct technical security audits of the agency as prescribed in the NCIC and NMLETS Operating

Manuals and the FBI CJIS Security Policy. These audits may occur at any time and/or for any or no reason, at the discretion of the DPS or any other appropriate entity.

3.4 ADVANCED AUTHENTICATION: The use of advanced authentication (example: smart cards or certificates and username/password) is required for certain methods of transmission (including but not limited to Wireless and Internet), and must comply with all rules, regulations, procedures and standards established in the FBI CJIS Security Policy for Criminal Information Networks.

3.5 ENCRYPTION: The use of encryption is required for all methods of transmission (including but not limited to Wireless, Internet, ATM and Frame Relay Circuits, etc.), and must comply with all rules, regulations, procedures and standards established in the FBI CJIS Security Policy for Criminal Information Networks.

3.6 EXECUTORY CLAUSE: It is understood by and between the parties hereto, that the *DPS* is obligated to provide services described in Section 3.1 above to *USER AGENCY* only to the extent that public and CISA funds are made available to the *DPS* for that purpose.

3.7 LOCAL AGENCY SECURITY OFFICER: *USER AGENCY* will designate an individual to serve as the Local Agency Security Officer (LASO) who shall be responsible for ensuring compliance with NMCJIS, CISA, and FBI CJIS Security policy and regulations. The individual selected as the Local Agency Security Officer for the *USER AGENCY* shall be identified on the final page of this document (refer to page 12), further noting that any changes to this designation must be communicated within five (5) working days to the NCIC Coordinator for the DPS, P O Box 1618, 4491 Cerrillos Road, Santa Fe, New Mexico 87507 or by calling 505.827.9181 or 505.827.3413.

3.8 TERM OF THE AGREEMENT

Either the *DPS* or *USER AGENCY* may terminate this agreement upon written notice to the other party, at least thirty (30) days before the intended date of termination. The *DPS* reserves the right to terminate service, without notice, upon presentation of credible evidence that the *USER AGENCY* is or has violated this agreement or any of the NCIC, NMLETS, NLETS Operating Manuals, and/or FBI CJIS Security policies.

IN WITNESS WHEREOF, the parties hereto have caused this agreement to be executed by the proper officers and officials.

DEPARTMENT OF PUBLIC SAFETY

BY: ______________________________
(Signature)

Jason R. Bowie
____
(printed name)

Cabinet Secretary
____
(title)

USER AGENCY

BY: ______________________________
(Signature)

____
(printed name)

____
(title)

DEPARTMENT OF PUBLIC SAFETY

BY: ______________________________
(Signature)

Jessica Rodarte for H.L. Lovato
____
(printed name)

State CJIS Systems Officer (CSO)
____
(title)

AGENCY DESIGNATIONS

TERMINAL AGENCY COORDINATOR

______________________________ Printed Name

______________________________ Office Phone Number

______________________________ E-mail Address

______________________________ Mailing Address

NM CJIS AGENCY COORDINATOR

______________________________ Printed Name

______________________________ E-mail Address

______________________________ Office Phone Number

LOCAL AGENCY SECURITY OFFICER

______________________________ Printed Name

______________________________ E-mail Address

______________________________ Office Phone Number

THE AGENCY MAY SELECT THREE INDIVIDUALS TO PERFORM THESE FUNCTIONS OR UTILIZE THE SAME INDIVIDUAL(S) TO PERFORM MULTIPLE FUNCTIONS.