



METER/NCIC

Directive 3 - 109

Date Issued: April 2016

Amends/Cancel: N/A

I. PURPOSE

This directive establish policy for access to and use of the Maryland Telecommunications Enforcement Resources System (METERS) which provides gateway access to National Crime Information Center (NCIC), National Law Enforcement Telecommunications Systems (NLETS) and the data files of the Motor Vehicle Administration (MVA).

II. POLICY

It is the policy of the Department of General Services Maryland Capitol Police (MCP) that criminal information systems as defined below are accessed and utilized by authorized members in accordance with applicable Federal and State laws, and all guidelines, rules, and regulations issued by the Maryland State Police and the Federal Bureau of Investigation.

III. DEFINITIONS

- A. CRIMINAL JUSTICE INFORMATION SERVICES (CJIS) - A computerized criminal justice information system that is a counterpart of FBI's National Crime Information Center (NCIC) and is maintained by Department of Justice (DOJ) in each state. It is available to authorized local, state, and federal law enforcement and criminal justice agencies via law enforcement communication systems such as NLETS, and METERS.
- B. NATIONAL CRIME INFORMATION CENTER (NCIC) - The National Crime Information Center (NCIC) is a computerized database of documented criminal justice information available to virtually every law enforcement agency nationwide, 24 hours a day, 365 days a year. The NCIC has been an information sharing tool since 1967. It is maintained by the Federal Bureau of Investigation (FBI) and is interlinked with federal, tribal, state, and local agencies and offices. NCIC is access though METERS in Maryland.
- C. MARYLAND TELECOMMUNICATIONS ENFORCEMENT RESOURCE SYSTEM (METERS) – This is the gateway through which all Maryland agencies have access to NCIC, Maryland's Hot Files, the MVA database, NLETS, etc.

IV. PROCEDURES

A. The Public Safety Article of the Annotated Code of Maryland empowers the Maryland State Police to establish rules concerning the use of METERS and sanction those agencies that violate the rules. Section 2-304 of the Public Safety Article states that: "Violation of a rule adopted under this subsection is a sufficient basis to withdraw permission to connect with and use the computer or communication system."

B. USE OF METERS, NCIC AND CJIS SYSTEMS

1. The use of the METERS, NCIC and CJIS systems are for official MCP business or communications and legitimate law enforcement purposes.
2. These systems are not to be used for political announcements and/or the dissemination of personal viewpoints. Any use of these systems by MCP employees for any personal reasons or for any other purposes other than those authorized by the MSP and the MCP is prohibited.
3. When certified METERS/NCIC operators run a criminal history, they must record:
 - a. the Originating Agency Identifier (ORI);
 - b. The following information regarding the subject of the inquiry:
 - (1) first/middle/last name;
 - (2) race, sex, and date of birth;
 - (3) FBI and State ID number of the requested record.
 - c. In addition, the operator will document:
 - (1) name, address and/or department of the person making the request;
 - (2) the operator entering the request, and;
 - (3) the purpose code;
 - (4) the reason for the request, i.e. incident report number, CAD record number, citation number, or traffic stop. The operator and requestor must be able to articulate just cause for the query.
4. Unauthorized use of the systems includes such things as:
 - a. running a check on a vehicle that an employee is interested in purchasing;
 - b. checking on a friend or neighbor to see if the individual has a criminal record;
 - c. or any other use that does not have a legitimate law enforcement purpose.

5. Any MCP employee found to be using or assisting another individual in using the METERS, NCIC or CJIS systems for personal reasons or for any purposes other than those authorized by the MSP and the MCP will be subject to disciplinary action and/or criminal charges.

C. TERMINAL AGENCY COORDINATOR (TAC)

1. The Maryland State Police, NCIC Audit Unit conduct annual audits of each agencies use of METERS/NCIC to verify that each requested criminal history has been run for a legitimate law enforcement purpose.
2. Each MCP Detachment, Division or Section assigned an ORI will designate one METERS/NCIC Operator as the Terminal Agency Coordinator (TAC) who will be responsible for facilitating the audit process.
3. The TAC will also be responsible for the monthly NCIC validation process and ensuring that all entries are validated and that the validation process is documented as required.

D. PHYSICAL SECURITY

1. Unauthorized access to METERS/NCIC terminals must be prevented.
2. The location of METERS/NCIC terminals and associated peripherals will be restricted to authorized personnel only.
3. Police vehicles with equipment which provides access to the METERS/NCIC must have adequate physical security at all times to protect against any unauthorized access or viewing.

E. HIT CONFIRMATIONS

1. When the MCP receives a hit confirmation request in response to an NCIC entry, the operator receiving the request must confirm the hit within 10 minutes for urgent requests, or one hour for routine requests, with the desired information.
2. Additionally, MCP personnel will confirm with the originating agency any NCIC record hit on a person or property inquired upon prior to taking any of the following actions based upon the hit:
 - a. Arresting the wanted person;
 - b. Detaining the missing person;
 - c. Seizing the stolen property;
 - d. Charging the subject with violating a protection order;
 - e. Detaining an individual where the record indicates the individual is wanted for extradition outside the State of Maryland.

F. CRIMINAL HISTORY RECORD INFORMATION (CHRI)

1. CHRI will only be disseminated to authorized personnel with criminal justice agencies for criminal justice purposes.
2. Authorized MCP personnel receiving a CHRI response shall record any secondary dissemination of the CHRI to another criminal justice agency, or an individual within another criminal justice agency, or to anyone legally entitled to receive such information that is not an employee of MCP.
3. The record of the CHRI dissemination shall be maintained for at least 24 months and shall be available for audit.