# DIRECTIVE 41.3 PATROL EQUIPMENT

Issue Date: 03/26/2020	By Order of Chief of Police
<b>Rescinds: (Issue 05/30/2019)</b>	CALEA Standards
	Referenced: 41.3.1; 41.3.2;
	41.3.3; 41.3.4; 41.3.5; 41.3.6;
Pages: 13	41.3.7, 41.3.8 & 41.3.9

# This directive consists of the following sections:

- 41.3.1 Patrol Vehicles Lights, Sirens
- 41.3.2 Equipment Specification/Replenishment
- **41.3.3 Occupant Safety Restraints**
- 41.3.4 Authorized Personal Equipment
- **41.3.5 Protective Vests**
- 41.3.6 Protective Vests/Pre-Planned, High Risk Situations
- **41.3.7 Mobile Data Access**
- 41.3.8 In-Car Audio / Video / Body-Worn
- 41.3.9 License Plate Recognition Systems

#### POLICY & PROCEDURE

In order for officers and/or employees of the Department to be able to deliver effective, efficient and high-quality law enforcement services to the community they must have access to the proper vehicles and equipment.

## 41.3.1 Patrol Vehicles Lights, Sirens

All vehicles used for routine patrol duties shall be equipped with an operational emergency light system, exterior spotlights, public address system and siren.

All vehicles used for routine patrol duties shall be conspicuously marked. The reflective markings shall include agency name, emergency telephone number, vehicle number and department emblem on the front left and right side doors and at a minimum have the word POLICE on both sides of the vehicle. The rear of the vehicle may be marked POLICE or Traffic Safety Unit.

#### 41.3.2 Equipment Specification/Replenishment

The following equipment shall be maintained in department vehicles used for routine patrol:

Mobile Data Computer

- In-Car Video/Audio System
- Radar Unit
- Fire Extinguisher
- First Aid
- Two Blankets
- Flashlight/Charger/Wand
- 10 Flares
- Evidence Collection Kit/Fingerprint Kit
- Lockout Tool
- Traffic Cones (4)
- Barrier Tape
- Two Clip Boards
- Heavy Duty Gloves (1)
- Hazmat Reference Book
- Deer Kill Receipt Slips
- Safety Throw Rope
- Floatation Vest
- Hobble Restraint
- Stop Sticks
- AR 15 (Patrol Only) (Spare Magazines in Go Bag)
- Measuring Wheel
- Spit Mask (Glove Box)
- PPE Kit
- Portable Breath Testing Equipment (In District & TSU Bags)
- Garage Remote & Gas/Car Wash Cards
- Transport Belts & Large Handcuffs (District Bag)

#### Additionally, Traffic Safety Unit vehicles shall be equipped with:

- Steel Measuring Tapes
- Traffic Cones (8)
- Traffic Code Book
- Inflatable Wedge
- Portable Breath Testing Equipment (In District & TSU Bags)

## Additionally, Supervisors vehicles shall be equipped with:

- Barrier Tape (Additional Roll)
- Large Volume OC Chemical Agent Unit
- Pry Bar
- Transport Belt
- Incident Command Board
- Red Man Helmet

Officers will be responsible for requesting supplies or equipment on a daily basis as needed. When an officer is aware that supplies or equipment are needed or in need of repair or replacement, they shall request repair/replacement via the Supervisor.

#### 41.3.3 Occupant Safety Restraints

Safety restraints shall be used by all persons riding in department vehicles any time the vehicle is in motion, except as provided for in the department's Prisoner Transport Directive 70.2.1.

#### 41.3.4 Authorized Personal Equipment

Miami Township Police Department issues all authorized personal equipment and apparel as listed in Directive 22.1.6. Officers may carry a department approved secondary firearm that is not supplied by the department. [4.3.1] No other apparel or equipment may be utilized.

# **41.3.5 Protective Vests**

The department purchases body armor for all officers. Body armor purchased must meet National Institute of Justice (NIJ) standards on the date it is purchased. All body armor vests shall be uniquely fitted for the individual officer to provide the best possible fit and coverage.

Uniformed patrol personnel, including bike unit and motorcycle officers are required to wear the department issued body armor when they are in uniform. Officers that are not on patrol and who are in the formal uniform or Honor Guard uniform are not required to wear the department issued body armor.

When personnel are representing the department and are authorized to wear civilian clothing, they are not required to wear the department issued body armor. Command Staff and Officers assigned to administrative duties are not required to wear the department issued body armor.

Should an officer be excused from wearing their body armor, the officer must have readily at hand their assigned body armor for use.

# 41.3.6 Protective Vests/Pre-Planned, High-Risk Situations

Investigative personnel could be exposed to situations which require arrest at any given time and without notice, therefore personnel working in that capacity are encouraged to wear body armor when actively working an investigation and must wear body armor when actively serving arrest warrants, engaged in a high risk operation or being part of a search warrant or raid. When the body armor is not being worn, the Detective shall have readily at hand their assigned body armor for use.

#### 41.3.7 Mobile Data Access

# <u>Guidelines & Restrictions – Mobile Data Computers</u>

It shall be the policy of the Miami Township Police Department to provide Mobile Data Computers (MDC) and associated equipment for the use of its officers assigned to road patrol and other duties, as resources permit. This equipment shall be used only for official purposes and within all established Miami Township, Clermont County, State of Ohio, LEADS/NCIC and NLETS rules and regulations.

Designated vehicles of the Miami Township Police Department are equipped with a Mobile Data Computer (MDC). The MDC is used to communicate with the communication center, communicate car-to-car, access the LEADS/NCIC network, write reports, and document work status.

The Clermont County Department of Public Safety, employed by the Miami Township Board of Trustees, is responsible for the day-to-day administration and security of the MDC system. Those responsibilities include:

- Monitoring of the System
- Installation and Removal of Software Products
- Installation and Removal of Hardware Peripherals
- Help Desk Operations
- System Security & Access

The Clermont County Department of Public Safety establishes access and issues password and login information to permit user access. Unauthorized introduction of software program or other files or the manipulation or alteration of current software running on the MDC is blocked via administrative rights access.

Miami Township Police Department in-house reporting software 'Interbadge' is installed on the MDC system. The Miami Township Police Department establishes access and issues password and login information to permit user access. Manipulation and alteration of this software is blocked via administrative rights access.

Training in MDC use is provided by Field Training Officers to new users upon their successful completion of the LEADS/NCIC certification test. Only certified LEADS/NCIC operators may be authorized to operate the MDC. Supervisors and FTO shall ensure that officers that are not certified for LEADS/NCIC access do not use the MDC equipment.

Use of the MDC is strictly limited to law enforcement related duties. MDC users accessing the LEADS/NCIC network via the MDC must adhere to established restrictions on use and dissemination of LEADS/NCIC information. Officers should not acknowledge the existence or non-existence of criminal records, traffic records, or any other information derived from the MDC to any person, group or organization, other than to another law enforcement officer.

Any transmission or reception (messaging, announcements, talk functions) via the MDC is considered to be a public record, subject to review or subpoena by the general public. The use of the MDC to transmit personal messages or personal email, or any other non-work-related text is strictly prohibited, and shall be grounds for disciplinary action. Supervisors with the Miami Township Police department may check, inspect, and evaluate any information, message or email sent or received by any Miami Township Police Department MDC user at any time.

The MDC is not to be used while the vehicle is in motion. Operators will stop and park the vehicle in a safe area prior to use.

Persons sitting in the patrol vehicle (passengers & prisoners) may be able to view data displayed on the MDC screen. Care must be taken to ensure law enforcement sensitive material and that non-law enforcement personnel do not view any LEADS/NCIC data. Officers shall give this security need special attention anytime a prisoner or observer is present in the police vehicle. When away from the MDC, operators will close the computer screen and lock the vehicle to secure the MDC.

Officers assigned to road patrol duties or special/selective enforcement grant funded opportunities will log onto the MDC before assuming an in-service status and logout just prior to the end of tour. This prohibits other persons from using your account for messaging or acquiring information. Officers assigned to other duties should log onto the MDC anytime that they expect to be in the patrol car for more than a few minutes. Officers will not operate an MDC assigned to another employee without consent of the Officer logged into the MDC.

If an officer loses their MDC password, he/she will notify the Clermont County Department of Public Safety (DPS) as soon as practical. Officers will leave a call back number and location so that a new password may be assigned. Passwords will not be issued via pagers or by third parties.

# Use of Mobile Data Computer

All traffic stops will be voice transmitted to the channel one dispatcher (Dispatch 1) for entry into the CAD system. After the dispatcher has entered the basic information into CAD system, the data will appear on the MDC in an "on scene" status. Officers may not use the MDC to call out on a traffic stop (to report a traffic stop). Officers may check "In Service" from a traffic stop via the MDC after adding a disposition to the stop.

After providing a license plate to the communications center, the dispatcher will check for wants/warrants and carry concealed license permits through LEADS and NCIC. If a hit is generated, the information will be voice transmitted by the dispatchers. Other information regarding the criminal/traffic history will be directed to the MDC for review. Clermont County Communication Center dispatchers set an alarm timer for all traffic stops, to alert the dispatchers to perform radio checks.

Officers receive all priority 1, 2, and 3 calls for service by voice transmission on channel 1, as well as delivered to the MDC. Upon receiving the call on the MDC, Officers will select the call given, mark the unit enroute to the call, and mark on the scene when they

arrive. Immediately after the call has been completed, the call will be closed and a disposition entered on the MDC.

Officers acting as back up unit(s) on a call for service or other activity also receive the information transmitted to the primary unit. Back up units must clear their "back up" status by using the available button on the MDC.

Low priority calls may be given directly to the MDC, and not by voice transmission. Examples include: returning phone messages, contacting another law enforcement agency, phoning headquarters, etc.

When entering data and or case summaries as well as reports for the Records Management System (RMS), Officers should check the spelling and accuracy of information. All levels of the criminal justice system, the news media and the public may review the information in the RMS. Reports will be reviewed for completeness and accuracy by supervisory staff.

Officers receiving a "hit" on a person, vehicle or article must notify the Clermont County Communication Center who will confirm the entry with the entering agency via LEADS, according to LEADS/NCIC policy and procedure. Officers will not take immediate action based solely on an MDC hit.

# Maintenance & Care of Mobile Data Computer

Officers are to keep the screen clean by using a soft cloth and using only accepted liquids for cleaning purposes. The screens are touch sensitive and subject to damage if abused. Drinks and other items that may damage the MDC are to be kept at a safe distance. Keeping the screen down and locked when not in use will prevent sun damage to the display and protect the keyboard. Magnetic objects or equipment that may generate an electro-magnetic field should be kept away from the MDC.

Operators will check the functionality of the MDC and screen before leaving on patrol or any assignment where an MDC equipped unit is deployed. Any failures and or damage will be reported to the on-duty supervisor as soon as possible.

Officers are responsible for proper care and use of the assigned MDC and may be held administratively and/or financially responsible in the event of negligent loss or damage of the MDC.

Problems with an MDC unit or repair needs shall be reported to the Support Services Supervisor.

## 41.3.8 Body-Worn and In-Car Audio & Video Systems

#### Purpose and Organization Philosophy Regarding Use

The use of body-worn audio/video recording devices (BWC) and in car cameras (ICC) in the operational police environment provides a potentially valuable resource for law enforcement agencies in the delivery of services. BWC's and ICC's allow for accurate documentation of police and public contacts, criminal investigations and critical incidents. They are useful while gathering evidence, showing probable cause, documenting contact with offenders and the arrest, release and transportation of an offender.

Audio and Video recording systems also serve to enhance the accuracy of officer's reports and testimony in court. Additionally, information collected through this technology can be useful during the investigation of complaints against employees.

#### Requirements and Restrictions for Activation and Deactivation

BWC and ICC equipment is issued primarily to uniformed personnel as authorized by this agency. Officers who are assigned BWC and ICC equipment must use the equipment while uniformed in a marked patrol vehicle unless otherwise authorized by supervisory personnel. Police personnel shall only use audio/video recording systems issued by our department and will only use the equipment in conjunction with official law enforcement duties. This policy does not govern the use of surreptitious recording devices used during undercover operations.

Officers shall activate the BWC and ICC systems to record ALL contacts with citizens in the performance of official duties upon receiving a call for service or engaging in official duty. The BWC and ICC system shall remain activated until the event is completed in order to ensure the integrity of the recording. During any call for service audio may be muted for discussion/briefs regarding tactics or strategies. When an officer activates the BWC or ICC he/she will also turn off the AM/FM radio inside the police patrol vehicle. BWC and ICC recordings are not a replacement for written reports

Officer safety and public safety take precedence over recording of events. Under extenuating circumstances, utilization of the BWC and ICC systems may not be possible; example: ambush, assault on a police officer, compromising the tactical advantage of the police.

Officers are not required to inform citizens they are recording an event and will not cease recording in the event the citizen requests it. Citizens shall not be allowed to review recordings at the scene.

If an officer fails to activate the BWC or ICC, fails to record the entire contact or interrupts the recording, the officer shall document why a recording was not made, was interrupted or was terminated. This documentation shall be included on the report supplement.

The BWC or ICC equipment shall not be used to record:

- Communications with other police personnel without the permission of the Chief of Police:
- Encounters with undercover officers or confidential informants;
- When on break or otherwise engaged in personal activities; or

- In any location where individuals have a reasonable expectation of privacy, such as a restroom or locker room *unless* the event is in the performance of official duties and it occurs in these locations;
- Inside an officer's home or residence, unless they are summoned there for a law enforcement purpose.

# **Traffic Stop Information**

When conducting a traffic stop officers should use optimum lighting at night whenever possible. Low beam headlights and takedown lights shall be used at a minimum. The spotlight should be directed at the area where the suspect is to be interviewed or given a field sobriety test. High beam headlights shall only be used when needed for officer safety. Overhead emergency pursuit lights and/or emergency flashers shall remain on for safety.

The officers' vehicle should be positioned approximately two car lengths behind the suspects' vehicle, in order to create a proper viewing area for interviews and for conducting field sobriety testing. If two car lengths are not possible, the officer shall adjust the camera angle to compensate for the shorter distance. Correct positioning of the camera will be done prior to exiting the patrol vehicle unless safety dictates otherwise.

Field sobriety tests/interviews should be done at the right rear of the suspect vehicle in full view of the video camera. If possible, field sobriety tests should not be conducted directly between the two vehicles. Standing between the suspect vehicle and patrol car can place the officer and suspect in a dangerous position if another vehicle crashes into the patrol car. The suspect should perform the field sobriety tests facing the patrol car with the officer standing at a forty-five-degree angle to watch the suspect and any occupants inside the suspect vehicle.

Officers shall try to keep the suspect in view of the camera if possible and consistent with the safety the conditions at the scene permit. When a suspect is placed in the patrol vehicle and/or when an officer transports a suspect from the scene, the ICC rear facing camera will be activated.

## School Resource Officer Information

School Resource Officers (SRO) will use BWC equipment pursuant to department policy when conducting official law enforcement duties, such as an arrest or involvement in a disturbance, and not during the ordinary course of the school day. Upon request, and if not otherwise prohibited by law, the Miami Township Police Department will provide the Milford Exempted Village School District with copies of SRO BWC recordings. Such copies will be maintained by the District as confidential student records pursuant to the Family Educational Rights and Privacy Act.

The regular use of a body worn camera as part of the School Resource Officers equipment is a law enforcement record that will be maintained and accessed according to

police department policy. The District and the Miami Township Police Department will confer and coordinate regarding requests for release of records that may implicate an exemption to Ohio public records law or federal and state student confidentiality laws prior to releasing the requested records to ensure compliance with all state and federal laws and regulations. A record that may constitute an infrastructure record of the school district is exempt from public records release as outlined in R.C. 149.433(B)(2). Miami Township Police Department will not release such records pursuant to a public records request.

Future state law enactments or state or federal case law may alter the status of BWC recordings made by SRO's in public schools, and if so, any such enactments or rulings will supersede this order upon their effective date.

# Criminal and Administrative Use of Camera Captured Data

The BWC and ICC equipment and all data, images, video and mega data captured, recorded or otherwise produced by the equipment is the sole property of the agency and are maintained on the evidence.com cloud storage site. Members of the department may not copy, publish, share or disseminate any audio, video, image or data to anyone expect as authorized by the department. Furthermore, members of the department may not edit, delete or alter any video or audio captured by the BWC or stored on the department's network or approved storage media without the written authorization and approval of the Chief or his/her designee. The requirement for written authorization does not apply in the case of a request for recordings originating from Prosecutor's Office employees or other law enforcement agencies as part of a court proceeding or an official investigation.

It is recognized that a use of force which results in the serious injury or death of a suspect may have an element of the investigation which could be handled by outside criminal justice agencies (i.e. Prosecutor's Office, Grand Jury Investigation), and this could be construed as a criminal investigation.

- An officer may review recordings as part of any casework or use of force investigation, to assist them with the completion of an accurate report.
- If a critical incident or use of force investigation involves serious injury or death of a suspect, the recording will first be viewed with the Investigations Lieutenant or the Chief's designee.
- Officers are restricted from viewing recordings in the event that criminal wrongdoing is overt and obvious.
- If an officer is suspected of wrongdoing which may result in criminal prosecution, the department reserves the right to limit or restrict an officer from viewing a video file.

Requests for deletion of portions of the recordings (i.e., in the event of a personal recording) must be submitted in writing and approved by the Chief or his/her designee in

accordance with state record retention laws. All requests and final decisions shall be kept on file.

Officers are encouraged to inform their supervisor of any recordings that may be of value for training purposes or civil litigation.

# Data Storage and Retention Requirements

All files shall be securely downloaded periodically and no later than the end of each shift. Each file shall contain information related to the date, BWC and ICC identifier and assigned officer. Routine recordings will be retained for a period of 90 days unless otherwise designated.

Files should be securely stored in accordance with state records retention laws and no longer than useful for purposes of training or for use in an investigation or prosecution. In capital punishment prosecutions, recordings shall be kept until the offender is no longer under the control of a criminal justice agency.

An officer may request that a BWC or ICC recording be archived and retained beyond the prescribed retention period. BWC and ICC recordings will be considered for archival if the recording is required for a criminal investigation/prosecution, internal investigation, pending civilian complaint, pending disciplinary matter or other circumstance deemed appropriate by the Chief of Police or his/her designee.

Biometric Searches: Stored video and audio from BWC shall not be used to create a database or pool of mugshots, for fillers in photo arrays, or searched using facial recognition software. This does not prohibit the agency from using recognition software to analyze the recording of an incident when the reasonable suspicion exists that a specific suspect or person in need of assistance may be a subject of a recording.

#### *Equipment Maintenance and Inspection Procedures*

BWC and ICC equipment is the responsibility of individual officers and will be used with reasonable care to ensure proper functioning. Officer will wear all supplied components of the BWC and ICC systems and ensure that it is properly positioned to record all events. Officers shall inspect and test the BWC and ICC prior to each shift in order to verify proper functioning.

Equipment malfunctions, damage, or a unit being unaccounted for shall be brought to the attention of the officer's supervisor as soon as possible. Supervisors shall conduct an immediate investigation when notified and make written documentation of their findings as well as action taken.

## Training Requirements for Users and Supervisors

Police personnel who are assigned BWC and ICC equipment must complete an agency approved and/or provided training program to ensure proper use and operations. Training

shall include a documented review of policy. Additional training may be required at periodic intervals to ensure the continued effective use and operation of the equipment and to incorporate changes, updates or other revisions in policy and equipment.

Newly hired personnel and personnel newly appointed to any supervisory capacity shall have documented training during field training. The documentation shall be made on the appropriate Field Training Task sign off sheet.

## Requirements for Documented Review of Camera Captured Data

At least bimonthly, the supervisor will randomly review fifteen minutes of each of the assigned officer's BWC and ICC recordings to ensure that the equipment is operating properly and that officers are using the devices appropriately and in accordance with policy and to identify areas in which additional training or guidance is required. This review shall be documented in Guardian Tracking.

# 41.3.9 License Plate Recognition Systems

#### Guidelines for Use

The Automatic License Plate Recognition (ALPR) consists of fixed cameras mounted on the light bar of selected marked vehicles, a USB cable located inside the passenger compartment and a program icon located on the ALRP terminal screen.

Any hits received through the ALPR including stolen vehicles, delinquent citations, or wants must be confirmed through dispatch, before enforcement action is taken. Officers shall also check the registration through LEADS before taking any enforcement action on a hit.

#### **ALPR Returns**

- Officers should notify the dispatcher via their radio prior to taking any action.
- Operators must confirm the plate by visually checking the actual plate against the captured image.
- After confirming the plate and the status of a wanted return, the operator may take enforcement action.
- After enforcement action is taken, a disposition should be entered into the ALPR system closing the incident.

# Data Security and Access

#### ALPR terminals shall not:

 Be used by persons other than trained members of this department. No member shall knowingly allow unauthorized access to Agency networks, systems or software.
 Passwords and access codes are to be protected from disclosure, distribution or viewing by unauthorized persons.

- Be stored in personal vehicles (point to point transport is allowed).
- Be connected to any device which allows connection to the 'Internet' without express written permission from the Chief of Police.
- Be charged of powered by an AC or DC Power supply/source which is not provided or approved by the Department.
- Be installed with any software executable program (whether it is licensed, shareware or freeware) without express written permission by the Department.
- Be installed with any executable 'screensaver' that has not been approved through the Department.
- Contain a 'desktop image' which depicts imagery deemed unofficial or inappropriate for public view. Desktop images other that the default one must have written approval from the Department.
- Have the systems configurations changed in any way.
- Have set passwords changed, bypassed, or used for access to system configurations of
  the system that are not normally meant for user access. No additional passwords may
  be created or encryption software installed which would prevent access or inspection
  to data files or systems within the ALPR system.
- Have any ALPR system designated 'audible alarm' or have 'tone' settings disabled, muted, turned off or otherwise tampered with.
- Be internally modified, upgraded or tampered with (changes or removal of RAM, Hard Drives, CD ROM Drives, Chipsets, Modems, or any other similar components) without express written permission by the Department.
- Be externally modified or tampered with consisting of modifications to hinges, latches, handles, lids, keypads and Department applied 'Property Number' decals and sticker which are to remain attached to the ALPR system and readable.
- Use the ALPR terminal to violate any security, privacy or confidentiality policies, or practices of the Department of Laws of the State of Ohio. The duplication, use or storage of any software that violates copyright provisions, violates license agreements or conflicts with existing network or application software is unauthorized.
- Be transferred or reassigned to another member without said reassignment being coordinated through the Patrol Division Supervisor.

#### **Operator Training**

No officer shall use the LPR equipment unless trained in use of the system.

## System Inspection & Activation

- Inspect the mounted cameras and USB Cable for damage.
- Power up the system by logging on to the ALPR terminal and clicking the ALPR icon located on the touch screen. Log in and select (Begin-Shift).

## System Shut Down

• Touch (End-Shift) which will download the captured information during the tour of duty.

• Log out of the system and verify the system is shut down before turning off the MDC.

## General Responsibilities

- ALPR terminals are intended to be used in conjunction with voice radio communications and are not intended to replace voice radio communications.
- Safe operation of the patrol vehicle is paramount. During solo (one officer only) patrol, common sense and safe driving practices dictate that the officer will focus his/her attention on safe operation of the vehicle and view the ALPR terminal screen only when the vehicle is not in motion.
- Information displayed on the ALPR terminal screen is confidential and caution shall be taken to ensure that unauthorized personnel do not view it.
- ALPR terminals should be in the 'VIDEO OFF' mode when a vehicle is temporarily vacant.

ALPR terminals shall be inspected by the user at the beginning of each tour of duty, while completing regular vehicle equipment checks. Any problems or damage shall be immediately documented and reported to a supervisor, who will forward the information through the chain of command to the Investigations Supervisor. The vehicle operator at the start of the tour shall be held responsible for any damage to ALPR terminal that is not immediately reported to a supervisor.

ALPR's shall be properly secured and protected from damage and theft. Terminals are not to be subjected to deliberate shaking, dropping, sliding, and excessive heat (such as caused by being stored in vehicle trunks). LCD Screens and Touch pads shall be protected from sharp objects that might cause damage. Use of touch pad stylus is permitted.

ALPR's are to be properly kept clean and free from: adhesives, stickers, ink, stains, liquids and debris (surface cleaning with a soft 'water only' damp cloth – no cleaning solutions). Food and beverage items shall not be placed on top of Terminal lids or keyboards. Crumbs, dust and debris shall be blown from or dusted from keypads. Sticky keys shall be reported and repaired by the radio technician.

## Data Storage and Retention

License Plate Recognition System data storage and retention is the responsibility of the City of Cincinnati.