OFFICE OF THE CHIEF OF POLICE

NOTICE
17.2

October 21, 2020

TO: All Department Personnel

FROM: Chief of Police

SUBJECT: ENHANCED DEPARTMENT SMARTPHONE CAPABILITY; REQUIRED MOBILE DEVICE SECURITY PROTOCOLS

The Department continues leveraging technology to provide new capabilities to officers in the field, including those which will increase officer safety and provide more efficient ways of policing. As part of that initiative, along with the updating or issuance of new Department smartphones, the following applications will soon be available to officers: PremierOne Handheld and NicheRMS. Both new applications require a secure connection to the Department's internal network, accomplished through Virtual Private Network (VPN) software and increased security protocols.

PremierOne Handheld

PremierOne Handheld compliments the features on Mobile Data Computers (MDC) in patrol vehicles to allow access to the Computer Aided Dispatch (CAD) system. With PremierOne Handheld, officers can complete many CAD-related functions from their smartphones including:

- View pending, stacked, and active radio calls;
- Update their unit status and monitor other units' status;
- Share location of handheld device, in addition to MDC location, on CAD mapping;
- Review comments of incidents;
- Initiate "Code-6" or traffic stops; and,
- Query vehicle, license, or warrant databases.

While logged into the PremierOne Handheld application (when deployed as a unit), the location of the handheld device will populate on the CAD mapping function. This functionality is expected to enhance situational awareness and officer safety in instances where an officer is away from his or her patrol vehicle.

NicheRMS

The NicheRMS application provides a mobile version of the Niche Records Management System (RMS) for convenient and accessible entry of data while in the field. The NicheRMS application supports initiating Investigative Reports, Field Interview Reports, and Traffic Collision Reports. An expansion for functionality to include citations and other reports is also under development.

Virtual Private Network and Increased Security Protocols

To provide the functionality of the two new applications, Department smartphones must securely connect to the Department's internal network. This secure connection is accomplished through a VPN client on the smartphone (software that creates a secure link) and increased security protocols that comply with Criminal Justice Information Services (CJIS) requirements. Among these new requirements, the Department smartphones are remotely managed (providing the ability to lock, securely wipe, or restrict application installation) and are set and locked to enable location services.

> **Note**: Although Department smartphones have location services enabled, it is not the intent of the Department to routinely monitor an officer's location beyond operational necessity or tactical officer safety reasons, without specific cause. Only the Information Technology Bureau smartphone administrators will be able to access the location of devices in real time when not logged into PremierOne Handheld.

Due to these additional security requirements, installation of third-party applications will be restricted and only enabled by Information Technology Bureau. Requests for an application to be added to the Department's Application Library can be sent to EnterpriseCybersecurityOperations@lapd.online. Applications will be subject to a security review. If the application passes the review, it will be added to the Application Library and available for download by all Department employees.

Procedures for Reviewing GPS Data for Incidents Investigated by Professional Standards Bureau (PSB) or the Multi-Disciplinary Collision Investigation Team (MCIT)

Officers or supervisors involved in an incident investigated by an entity within PSB or MCIT shall not be allowed to review GPS data until authorized to do so by the assigned investigative supervisor. Officers or supervisors will, however, be allowed to review the relevant GPS data prior to being interviewed or providing a written statement. Officers may have an employee representative present during the review of GPS data without the PSB or MCIT investigator or supervisor present. In any incident investigated by PSB or MCIT, the review of GPS data shall not occur jointly among the involved officers. In a Categorical Use of Force incident, the separating and monitoring of officers involved shall be maintained during the review of the GPS data, subject to the ability of the officer conferring with a representative privately.

If you have any questions regarding this Notice, please contact Information Technology Division, at (213) 486-0844.

MICHEL R. MOORE
Chief of Police

DISTRIBUTION "D"