

## **JUSTICEMOBILE PROGRAM SUPPORT**

**0970**

(June 1, 2015)

JusticeMobile is a mobile web application service delivered by the California Department of Justice (DOJ) to its law enforcement agency partners. JusticeMobile gives law enforcement agents secure and immediate access to State and Federal criminal justice information.

### **REFERENCE(S)**

**0970.1**

(June 1, 2015)

Criminal Justice Information Services (CJIS) Security Policy Version 5.3 (8/4/2014)  
National Crime Information Center (NCIC) Operating Manual  
[Title 28, Code of Federal Regulations, Part 20](#)  
California Law Enforcement Telecommunications System (CLETS) Policies, Practices, and Procedures (PPP) (Rev. 03/2013)  
[CAL FIRE 9400 Law Enforcement Handbook](#)  
[CAL FIRE 0900 Information Technology Services Handbook](#)  
[State Administrative Manual Section 5300 et seq.](#)

### **GENERAL PROVISION**

**0970.2**

(June 1, 2015)

CAL FIRE utilizes JusticeMobile and its accompanying Mobile Device Management (MDM) service through DOJ to provide the means of securing, connecting, and presenting Criminal Justice Information (CJI) in accordance with the CJIS Security Policy requirements on approved mobile devices and in compliance with the CLETS PPP.

JusticeMobile provides inquiry only access to CJI in the statewide databases of the California DOJ, California Department of Motor Vehicles, and others as well as access to interfaces with the Federal Bureau of Investigation's (FBI's) NCIC databases on mobile devices.

Access to JusticeMobile and/or CLETS is controlled by the DOJ and administered by CAL FIRE's Law Enforcement Program. Only authorized personnel may access the data and/or systems. Anyone violating this control by using an end users password or other means to gain unauthorized access will be subject to disciplinary action and possible criminal prosecution.

Authorized users are responsible for ensuring that they follow the stipulations outlined under the “Reference(s)” section above in addition to any other applicable standards (e.g. CAL FIRE’s Acceptable Use Policy) regarding access, use of data, and protection of data. CAL FIRE Law Enforcement Program shall maintain copies of authorizing documents and will maintain inventories for mobile devices issued under this program.

Annual CLETS compliance training shall be completed by all authorized users.

Questions regarding administration of the JusticeMobile Program for CAL FIRE should be directed to the Department’s Agency Head as defined by DOJ (i.e. Staff Chief, Law Enforcement) and/or CLETS Coordinator (i.e. Deputy Chief, Law Enforcement).

JusticeMobile use is subject to review and approval by DOJ’s CLETS Administration Section through the standard CLETS application process and subject to audit.

## **PROCEDURES**

**0970.3**

(June 1, 2015)

### **Mobile Device Support**

CAL FIRE Information Technology Services (ITS) support personnel will only support the system software and configurations that are designed to control access to CLETS on a mobile device. At no time should ITS support personnel access the CLETS application itself, or view CLETS information.

The DOJ employs a 24x7 support program for the JusticeMobile application and associated MDM software. For assistance with the JusticeMobile application or CLETS data employees should call the DOJ Help Desk at (916) 227-2256. For password resets contact the DOJ “BUD” Hawkins Data Center (HDC) at (916) 227-3000.

### **Secure Mobile Computing**

DOJ JusticeMobile and MDM provide the secure mobile computing environment that appropriately protects CJI on dedicated devices. However, authorized users must be aware of other risks associated with mobile devices.

**Significant risks in connecting to public wireless access points make this activity prohibited on devices which have the JusticeMobile application installed.** Rogue access points masquerading as legitimate public access points may allow for man-in-the-middle, eavesdropping, and session hijacking attacks. Mobile devices connecting to foreign cellular networks and/or used outside of the United States require special handling.

Mobile devices utilizing Bluetooth, including the data device itself, and any authorized Bluetooth accessories associated to the device, must meet CJIS Security Policy Bluetooth requirements, including Departmental standards.

Device integrated chat/texting applications and many common third-party chat applications should not be considered secure or appropriate for transmission of CJI data. Texting functions that utilize a cellular providers Short Message Service (SMS) or Multimedia Messaging Services (MMS) functions do not constitute a secure transmission medium.

Questions regarding secure mobile computing should be submitted to the Department's CLETS Coordinator within ITS Customer Services Unit.

### **Physical Security**

Mobile devices that cannot be carried on the authorized individual's person have an increased risk of intentional device theft from vehicles and/or unsecure locations. Physical protections are the responsibility of the assigned authorized user.

### **Incident Response**

Loss of device control (i.e. device is in the physical control of a non-CJIS authorized individual or the device is left unattended in an unsecure location even if the device is recovered quickly), total loss of the device, and/or potential device compromise (e.g., rooting, jailbreaking, or malicious application installation on device) **must be reported immediately**, but no later than 24 hours to the respective Bureau Chief and Security Point of Contact (SPOC) (i.e., Information Security Officer/Privacy Protection Coordinator).

The SPOC, working in conjunction with the Agency Head, CLETS Coordinator, and ITS, is responsible for DOJ incident reporting. The CAL FIRE 0900 Information Technology Handbook Section 0938 on information security incident reporting remains applicable with additional reporting requirements by DOJ.

[\(see HB Table of Contents\)](#)

[\(see Forms or Forms Samples\)](#)