

OFFICE OF CHIEF OF POLICE
OAKLAND POLICE DEPARTMENT

MEMORANDUM

TO: All Personnel

DATE: 15 Dec 09

SUBJECT: Departmental General Order I-14, COMPUTERIZED POLICE
REPORTING (Rev. 27 Oct 06)

The subject order has been revised to update Departmental policy and procedures for Field Based Reporting (FBR), a computerized method of writing police reports, through the use of mobile data terminals (MDT) and authorized Departmental computers. Updates include revisions to definitions, policy, responsibilities, WiFi Hotspots, and support; new protocols for authorized users and supervisors; password creation; reporting lost or damaged laptops; system-wide malfunctions/failures;

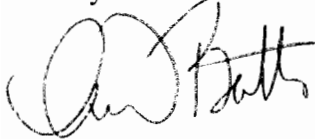
The Evaluation Coordinator for this order shall be the Bureau of Field Operations Deputy Chief, who, without further notice, shall forward the required report to the Chief of Police on or by 15 Jun 10.

The Evaluation Coordinator shall receive, review and document the acceptance or rejection of all comments and/or recommendations received prior to submitting his/her six-month evaluation report.

The Evaluation Coordinator shall forward a copy of the six-month evaluation report, along with the comments/recommendations received, to the Office of Inspector General to be maintained in the appropriate Departmental General Order archive folder.

Personnel shall acknowledge receipt, review, and understanding of this directive in accordance with the provisions of DGO A-1, DEPARTMENTAL PUBLICATIONS

By order of



Anthony W. Batts
Chief of Police

Date Signed: 12/10/09



DEPARTMENTAL
GENERAL
ORDER

Effective Date
15 Dec 09

I-14

Evaluation Coordinator:
BOS Deputy Chief

Index as:

Evaluation Due Date:
15 Jun 10

Computerized Police Reporting

Automatic Revision Cycle:
3 Years

COMPUTERIZED POLICE REPORTING

The purpose of this order is to set forth Departmental policy and procedures for Field Based Reporting (FBR), a computerized method of writing police reports, through the use of mobile data terminals (MDT) and authorized Departmental computers.

I. DEFINITIONS

- A. Authorized Users – OPD personnel trained to prepare reports using the FBR software.
- B. Field Administrator – Specially trained OPD personnel capable of restoring reports in “Out” status to the main server.
- C. “Report Grid” – The database, located on a secure server, that stores all of the FBR report files created using the FBR software by authorized users. The Report Grid contains the following categories of reports:
 - 1. “Open” – The status of a report that is “in progress” mode. The report can be sent to and retrieved from the server and then edited (can be edited only by the author).
 - 2. “Copy” – A read-only duplicate version of a report. Copies are created when an Approved, Finalized, or Out status report is requested.
 - 3. “Done” – The status of a report that has been completed, but not yet finalized, failed, or approved. The report can be sent to and retrieved from the server and then edited (by the author only).
 - 4. “Final” – The status of an approved Field Interview report.

5. “Fail” – The status of a report that is incomplete or needs modifications. Only an authorized reviewer may “fail” a report.
 6. “Out” – Status of a Done or Open report that has been retrieved (checked out) from the server. Reports may be restored to the server by an authorized administrator, but all unsaved edits/approvals will be lost.
 7. “Approved” – The status of a report that has been confirmed/certified by a reviewer (author/supervisor/commander).
- D. “WiFi Hotspot” – A specific geographic area or access point where an MDT or laptop can utilize a restricted high-speed radio transmission (Appendix).
- E. “EVDO” card – An internal or external aircard which allows a laptop to access the network via a cellular backbone while roaming.
- F. Mobile Data Terminal (MDT) – A permanently installed in-car computer.

II. POLICY

- A. An authorized MDT, laptop or Departmental desktop computer shall be used as the primary method of drafting an electronic report using FBR software.
- B. Field personnel shall seek supervisory approval to use a designated Departmental desktop computer for drafting and submitting a report if any of the following conditions exist:
 1. Multiple authorized users (i.e., Adam unit) need to utilize the same MDT/Laptop at the same time to draft individual electronic reports.
 2. The MDT/Laptop is not functional; or
 3. There is no access to the network via EVDO or a “Hotspot.”
- C. If the FBR system is not functioning, OPD personnel shall prepare reports on the appropriate hardcopy forms, with prior supervisory approval.
- D. Use of the “WiFi Hotspots” is restricted to OPD MDTs/laptops only.

- E. In the event of an EVDO aircard failure, FBR files shall only be uploaded and downloaded at designated City WiFi Hotspots or at designated Departmental desktop computers.

NOTE: WiFi locations allow MDTs and laptops to receive updates and upgrades more quickly than the EVDO aircards.

- F. MDTs and laptops shall be maintained and configured by authorized personnel only. No unauthorized user shall tamper with or modify any MDT, laptop, Department desktop computer, or WiFi software/hardware devices in accordance with the provisions of DGO I-1.
- G. All users shall use a secure password that complies with the protocols prescribed by the Criminal Justice Information Services (CJIS)¹. All passwords shall meet or exceed the following standards and shall not be shared:
1. Passwords shall be a minimum length of eight (8) characters and a maximum of fifteen (15) characters, and include at least one (1) numeral OR special character (e.g., #, \$, %, &, *, +).
 2. Passwords and the User ID shall not be the same.
 3. Users shall create a new unique password every 90 days. Password reuse (any of the last 10 passwords) is prohibited
 4. Passwords shall not be transmitted, shared, or revealed to others.
- H. Authorized User Responsibilities

Authorized users:

1. Shall only conduct official police business on an OPD MDT, laptop, and Department desktop computers in accordance with DGO I-1.
2. Shall report any MDT/Laptop or FBR system interruption in accordance with the provisions of Part VI of this order.

¹ CJIS Security Policy Section 7.3.3

3. Shall not configure a personally-owned laptop computer for use on the WiFi network.
4. Shall not disclose the locations of the WiFi access points to any unauthorized person.
5. Shall care for property and report lost and damaged property in accordance with DGOs I-1, Personal Computers and Electronic Messaging Devices; N-5, Lost, Stolen, or Damaged City Property; and Manual of Rules Sections 342.00 and 342.19.

III. RESPONSIBILITIES

- A. FBR System Administrators – Designated by the Bureau of Services Deputy Chief.

Responsibilities:

1. Application and Account Management
 - a. Serve as Departmental liaison between OPD and City of Oakland Department of Information Technology (DIT) for problem resolution and system management;
 - b. Ensure the FBR system is maintained and functioning properly;
 - c. Troubleshoot, track and report system problems appropriately and recommend system upgrades and modifications;
 - d. Develop and evaluate relevant Departmental policy and procedure publications and manuals;
 - e. Ensure system upgrades are tested, implemented and coordinate training;
 - f. Maintain authorized user list and manage passwords;
 - g. Prepare and submit to Command Staff a report of "Done" and "Open" reports upon request.
 - h. Coordinate with organizational units regarding FBR issues.

2. Coordinate Training

- a. Assess and identify training needs for end users;
- b. Develop relevant training for end users;
- c. Create appropriate training documentation;
- d. Identify authorized trainers; and
- e. Coordinate training delivery with the Training Section.

B. Field Administrator – Designated by the Bureau of Services Deputy Chief

Responsibilities:

1. Restore “Out” reports to the main server not appropriately returned (sent up). All unsaved edits or approvals made on the local computer will be lost upon restoration.
2. Field test new/upgraded hardware/software, and procedures as needed;
3. Report problems and suggest enhancements as needed.

C. Authorized Users

1. Authorized users (authors) shall complete a report utilizing the FBR system and:
 - a. If the report does not require supervisory approval, finalize the report and send to the server; OR

If the report requires supervisory approval (refer to DGO M-18), send the “Done” report to the server and notify his/her supervisor of a pending report needing approval. If the author’s immediate supervisor is not available, the user shall notify another on-duty supervisor of a pending report needing approval. Authors shall stand-by until an in-custody report is approved by the notified supervisor/commander.

- b. If the report is marked as “Fail” by the reviewer, the author shall make the necessary corrections/revisions to the report as directed, place the report back in “Done” status, and re-submit the corrected report for approval, as outlined in a) above.
2. Authorized users shall review the FBR system for “Fail”, “Done”, “Open”, or “Out” reports at the beginning of his/her tour of duty, and take the following actions:
 - a. “Fail” reports shall be revised/corrected, placed back into “Done” status, and re-sent to the server for approval.
 - b. “Done” reports shall be evaluated for further edits or approvals and handled appropriately.
 - c. “Open” reports shall be evaluated for further edits and handled appropriately.
 - d. “Out” reports are stored on the local computer and shall be sent to the server from that computer, in order to preserve any edits made. In the event the local computer cannot be identified, the user shall notify an authorized FBR Field Administrator to restore the report to the server.

D. Supervisors

Supervisors shall:

1. Review the Report Grid daily to ensure subordinates’ “Open”, “Done”, and “Out” reports are properly processed.
2. For reports requiring supervisory approval, retrieve and review subordinates’ “Done” reports and take the following actions:
 - a. If the report is complete and does not require revision, “Approve” the report and return to the server; or
 - b. If the report is incomplete and/or needs revision, return the report to the server in “Fail” status and notify the author.

NOTE: Approval authority is granted upon appointment to a supervisory position or upon certification to be an acting sergeant. Persons who are certified as acting sergeant shall use their approval authority only while actively serving in a supervisory capacity.

E. Traffic Investigators

All Traffic Accident Reports shall be reviewed and approved by authorized Traffic investigators only.

Traffic investigators shall review the Report Grid daily for all "Done" Traffic Accident Reports and take the following actions:

1. If the report is complete and does not need revision, "Approve" the report and return to the server; or
2. If the report is incomplete and/or needs revision, return the report to the server in "Fail" status and notify the author.

F. Report Reproduction Unit

Designated Report Reproduction Unit (RRU) staff shall refresh and view the LRMS "Mobile" queue within the "To Be Entered CAD" queue a minimum of once per RRU shift and process FBR reports in accordance with the provisions of Departmental General Order M-2, REPORT PROCESSING AND DETAILING.

G. Criminal Investigation Division

Each section commander or designee shall view the LRMS "To Be Assigned" queue and assign investigative cases in accordance with the provisions of Bureau of Investigation Policy and Procedure 00-02, Case Screening.

IV. WIFI HOTSPOTS

- A. The attached map displays the 18 WiFi Hotspots within the City of Oakland. These Hotspots are part of a secure system and are only accessible to the OPD and OFD vehicles equipped with MDTs or laptops.
- B. WiFi locations shall be used to log-on to the MDTs or laptops;

V. SUPPORT

- A. In the event of an occurrence of power outage, WiFi Hotspot connection problem, or an MDT malfunction, the user shall contact the City of Oakland Department of Information Technology (DIT) Help Line at 238-2000 or by emailing helpdesk@oaklandnet.com immediately, but no later than 24-hours. Leave the following information with the Helpdesk representative or on voicemail/email:
1. Name;
 2. Contact information;
 3. A brief description of the problem; and
 4. Location of the equipment or vehicle (i.e., PAB, Eastmont Precinct, and associated vehicle number (if needed).
- B. Laptop malfunctions or damage shall be reported to:
1. City of Oakland Department of Information Technology (DIT) Help Line at 238-2000 or by emailing: helpdesk@oaklandnet.com; or
 2. OPD Information Technology Unit at 510-238-7192 or by emailing: opditu@oaklandnet.com.
- C. In the event of a system-wide failure, contact the Communications Section who shall request priority City ITD technician service.

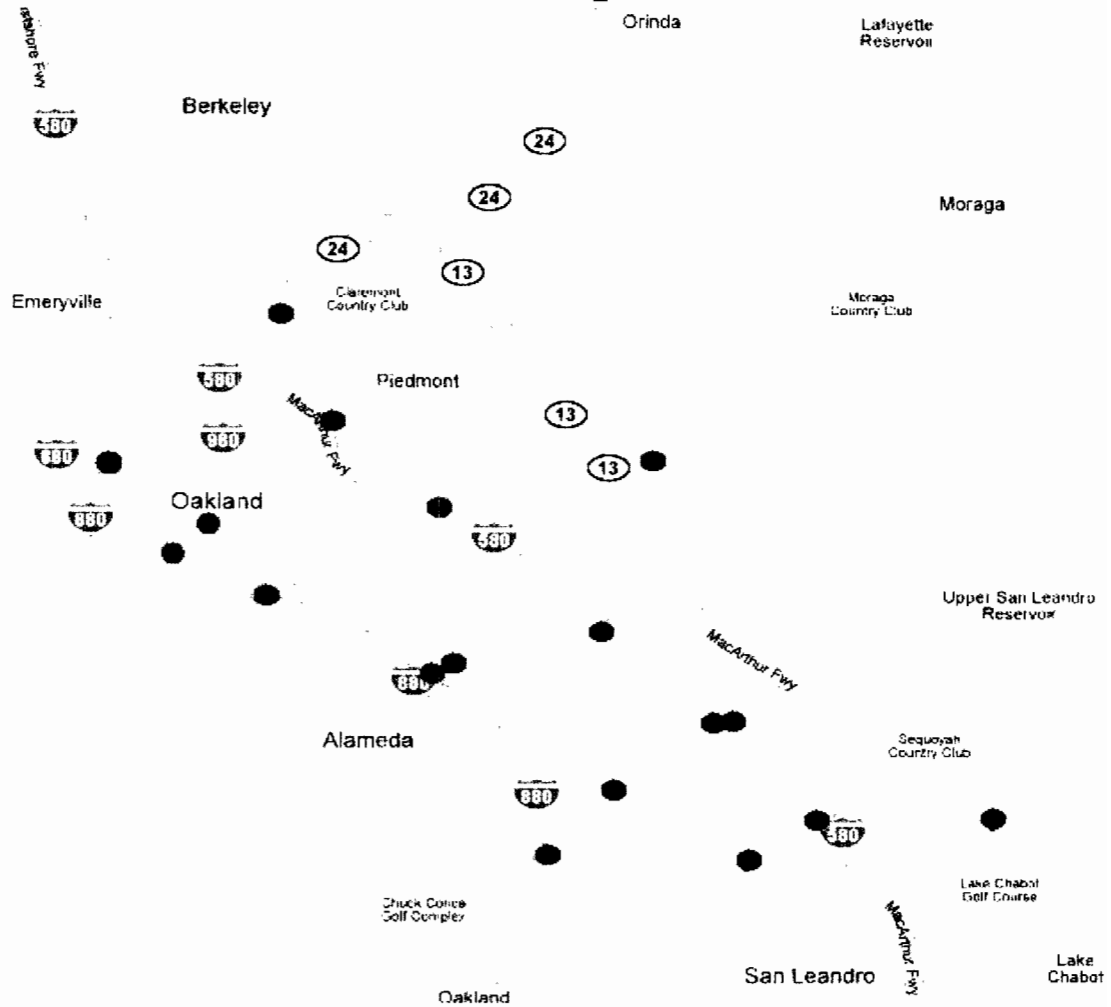
By Order of



Anthony W. Batts
Chief of Police

Date Signed: 12/10/09

APPENDIX Oakland Police Department WiFi 18 Hot Spot List



PSA 1

- OPD Transportation - 455 7th St.
- OPD Sta 02 Fireboat - 100 Jack London Square
- OPD Station 03 - 1445 14th St

PSA 2

- OPD Station 08 - 463 51st St
- OPD Station 10 - 172 Santa Clara Ave

PSA 3

- OPD Taxi Detail - 8th Ave & Embarcadero
- OPD Station 16 - 3600 13th Ave

PSA 4

- Fruitvale Substation - 1101 29th Ave
- OPD Station 13 - 1225 Derby Ave
- OPD Ranger Station - 3590 Sanborn Drive

PSA 5

- OPD Eastmont Precinct - 2651 73rd Ave
- OPD Eastmonth - Lower - 2651 73rd Ave
- OPD Station 29 - 1016 66th Ave
- OPD Station 17 - 3344 High Street

PSA 6

- OPD Station 20 - 1401 98th Ave
- OPD Station 26 - 2611 98th Ave
- OPD Corp Yard #1 - 7101 Edgewater
- OPD Station 28 - 4615 Grass Valley Rd