UCLA POLICE DEPARTMENT

RECORDS MANAGEMENT

AUDIT REPORT #18-2210

Audit & Advisory Services

July 2018

UCLA POLICE DEPARTMENT

RECORDS MANAGEMENT

 AUDIT REPORT #18-2210

# Background

In accordance with the UCLA Administration’s fiscal year 2017-18 audit plan, Audit & Advisory Services (A&AS) performed an audit of the UCLA Police Department’s (UCPD) records management activities. The Records Unit is responsible for recording, storing, safeguarding, releasing, and disposing of police reports, citations, and various forms. The Records Unit also provides fingerprinting services to University departments and the surrounding community.

UCPD records are captured and maintained electronically and in paper format, depending on the type of record. Incident and crime reports, arrest reports, and traffic collision reports are captured and maintained electronically in the Records Management System (RMS). RMS is one of the modules of a suite of public safety software offered by a vendor called Superion. Other modules utilized by UCPD include Computer Aided Dispatch and Mobile Field Reporting. RMS software was implemented in 2012. There are still some paper records maintained such as parking citations, vehicle moving violations, vehicle towing forms, and lost property reports.

The Records Unit is required to comply with various state and federal laws, policies, and guidelines such as the Criminal Justice Information Services (CJIS) Security Policy and National Crime Information Center (NCIC) to ensure their records are valid, complete, and accurate. The Department of Justice (DOJ) conducts on-site audits to verify compliance with these requirements. The most recent DOJ audit was conducted in September 2016, during which UCPD was found be to in compliance with CJIS and NCIC requirements. In addition, the Records Unit must comply with the California Public Records Act which requires law enforcement agencies to provide information the public has the right to know, while restricting the release of certain information to protect individual privacy, safety, and reputation. Furthermore, there are federal, state, and University laws and guidelines for the retention of criminal justice records.

For fiscal year 2016-17 UCPD processed approximately 2,700 police reports and 1,700 citations. The Records Unit is comprised of a Records Manager and four records management clerks. The Records Manager reports to the Administrative Division Lieutenant. The Chief of Police oversees UCPD.

# Purpose and Scope

The purpose of the review was to ensure that UCPD’s organizational structure and controls are conducive to accomplishing its business objectives with regards to records management activities. Where applicable, compliance with University policies and procedures was also evaluated.

The scope of the audit focused on the following:

* Accuracy, Completeness, and Timeliness of Records
* Access to Records
* Availability of Records
* Release of Records
* Records Retention

The review was conducted in conformance with the International Standards for the Professional Practice of Internal Auditing and included interviews, tests, and other procedures considered necessary to achieve the objective.

# Summary Opinion

Based on the results of the work performed within the scope of the audit, UCPD’s structure and controls are generally conducive to accomplishing its business objectives as they pertain to records management activities. However, control processes could be further strengthened by implementing the following:

*Access to Records*

* UCPD management should periodically review the RMS user listing, and ensure that RMS access is disabled for employees who transfer or separate from the department.

*Availability of Records*

* UCPD management should perform a business impact analysis and identify how timely RMS would need to be recovered in the event of a disaster, and establish a plan that will meet their recovery time objectives. As part of their overall disaster recovery planning efforts, management should also assess if backups should be stored at a more distant location away from campus.

*Release of Records*

* The Records Unit should consider revising the "Application for Release of Information" form to require that the following additional information be documented: person authorizing the release, person releasing the report, date report was released, if a fee was collected or waived, and if a request is denied, the reason why.
* UCPD management should remind staff that the reason for printing and releasing reports should be clearly documented.

*Records Retention*

* UCPD management should update their records retention schedule and ensure that their records are retained or disposed in accordance with current laws, regulations, and University policies.

The audit results and recommendations are detailed in the following section of the report.

Audit Results and Recommendations

Accuracy, Completeness, and Timeliness of Records

After an incident is reported, the police officer is responsible for creating a police report in the Mobile Field Reporting system. The police officer is responsible for ensuring that all pertinent information is adequately documented, such as including the person(s) involved with the incident, the location of the incident, selecting the correct penal and Uniform Crime Reporting (UCR) codes, and writing a narrative of the incident.

When completed, the police officer must electronically sign-off on the report. The police reports must then be reviewed by a supervisor for accuracy and completeness, including confirming that the penal and UCR codes are correct, that the narrative makes sense, and that all required information is recorded. Review notes are communicated electronically through the system to the police officer.

When all the review notes are addressed, a supervisor will approve the report. The report is then uploaded to the RMS queue for review by the Records Unit, who double-check that all required information has been recorded, and that the penal and UCR codes are correct and correspond with the narrative. Once approved by the Records Unit, the report is locked and modifications can only be made by adding supplemental documents to the report.

1. Incident Reports

Patrol lieutenants receive a weekly report of missing incident reports and unfinished supplemental reports, and are responsible for following up with the police officers to ensure that the reports are completed. According to the missing incident reports and unfinished supplemental reports as of October 26, 2017, there were 31 incident reports noted as not started.

Approximately 2,700 incident reports were completed during 2017, according to the Investigations Unit Lieutenant, thus only 1% of the incident reports were not started.

A judgmental sample of five missing incident reports were selected to determine if there are valid reasons why the reports are missing. A&AS discussed the reports with the Patrol Lieutenant, who indicated that all five incidents were cancelled and thus incident reports were not required. The Patrol Lieutenant also indicated that they are working on updating the status for reported incidents that are subsequently cancelled, so they no longer are included on the weekly missing incident reports.

There were no significant control weaknesses noted in this area.

1. Police Reports

Police reports are expected to be completed by police officers by the end of their shift or the end of the work week, depending on the type of report. Once a police officer completes a report, their supervisor is expected to review the report within the same day. The Records Unit’s goal is to review police reports within two business days after the supervisors approve the reports.

A judgmental sample of ten incidents reported during fiscal year 2016-17 were reviewed, noting the following:

* Seven reports were completed and approved by a supervisor the same day the incident was reported, two reports were completed the following day, and one report was completed in three calendar days.
* With regard to the Records Unit's review, six reports were reviewed within their goal of two business days; however, four reports were reviewed up to five to 21 business days later. It should be noted that the Records Unit has been short-staffed.
* Incident reports were reviewed by a supervisor and the Records Unit for accuracy and completeness.
* The police officer writing up the police report is responsible for selecting the correct penal and UCR codes, based upon the reported incident. Supervisors and the Records Unit are responsible for checking that the UCR codes selected are correct. All the UCR codes selected and reviewed within the judgmental sample of the ten incident reports appeared to be correct.

There were no significant control weaknesses noted in this area.

Access to Records

UCPD records are captured and maintained electronically and in paper format, depending on the type of record. Incident and crime reports, arrest reports, and traffic collision reports are captured and maintained electronically in RMS. There are still some paper records maintained such as parking citations, vehicle moving violations, vehicle towing forms, and lost property reports. The following were noted in reviewing access to RMS:

1. Disabling User Access – Separated Employees

A&AS verified that access to RMS is disabled for employees who transfer or separate from the department, by comparing the RMS user listing to a listing of all the active employees in UCPD. Of the 101 RMS user accounts directly associated with employees (not including generic accounts), 95 belong to active UCPD employees, three are to employees out on leave, and three were former employees who have separated from the University.  The separation dates for the three employees were March 2015, April 2016, and October 2017.

Recommendation: UCPD management should periodically review the RMS user listing, and ensure that RMS access is disabled for employees who transfer or separate from the department.

Response: Concur. System access will be removed for separated and transferred employees. The department will periodically review the RMS system to ensure only appropriate individuals have access.

1. User Authentication

User authentication to RMS was reviewed and discussed with UCPD management. Test work indicated a valid user ID and password is required to access RMS.  Passwords must be at least eight characters, cannot include repeating characters, and should contain three of the following conditions: lower case, upper case, numeric, special characters.  New passwords cannot match the ten previous passwords.  User accounts are set to lockout after three consecutive invalid login attempts.  In addition, user workstations are locked after ten minutes of inactivity.

There were no significant control weaknesses noted in this area.

1. User Access – Security Groups

User access to RMS was reviewed to verify that access is restricted based upon an employee’s job title and responsibilities.  For example, there are security groups for police officers, detectives, Emergency Medical Services (EMS), and Records Unit staff, each having different levels of access to RMS.

Utilizing data analytics, A&AS verified for all 113 of the RMS user accounts (including generic accounts), that the security groups assigned were consistent with the employees’ job titles. Audit review indicated that there were six user accounts with assigned security groups that were different than their job title.  These user accounts were reviewed with the UCPD Information Systems (IS) Manager, who indicated the security groups assigned are appropriate and are required based upon their job responsibilities.  There was one user assigned additional access to help test a new feature of RMS; however, the access was not removed after the testing was completed. The UCPD IS Manager has since removed the additional access.

There were no significant control weaknesses noted in this area.

1. System Administrators

System administrator level access to RMS was reviewed and discussed with the UCPD IS Manager, noting that access is restricted to limited, authorized personnel, whom require system administrator level access, based on their job responsibilities.

There were no significant control weaknesses noted in this area.

1. Vendor Access

The software vendor’s access to RMS was reviewed and discussed with the UCPD IS Manager. The software vendor has remote access to RMS for support and troubleshooting purposes. Remote access is controlled through a software called SecureLink Gatekeeper. Each vendor support technician has their own unique login credentials. Every time the vendor connects remotely, an e-mail is automatically sent to the UCPD IS Manager, which includes the following information: name of the specific vendor technician that connected to RMS, start time and end time of connection, description of the work performed, and the support ticket or work order number.

There were no significant control weaknesses noted in this area.

1. User Accountability and Audit Logs

The RMS user access listing was reviewed to verify that users are assigned unique user IDs. For any generic accounts, A&AS staff reviewed and discussed these with the UCPD IS Manager to determine if there is user accountability when the accounts are used.

Regular RMS users are assigned unique usernames. There are six generic user accounts that are used when police officers from other campuses help provide mutual aid at UCLA. Each mutual aid officer is assigned one of the six generic accounts, ensuring that multiple individuals do not share any one account.  There are two other generic accounts that are only used for training purposes.  Lastly, there was one generic account (crime analyst with temporary access), which was no longer needed and was disabled by UCPD.

Logging of all user activity in RMS was discussed with UCPD management and examples of audit logs were reviewed. Test work indicated that user activity in RMS is logged, including who accessed, edited, deleted, or printed any records or reports and the log is available for review when necessary.

There were no significant control weaknesses noted in this area.

1. Server Room Security

A&AS observed the RMS server room with the UCPD IS Manager and verified the physical security controls in place. The server room is located in the UCPD building on the second floor.  Access to the office area where the server room is located is restricted to UCPD employees via a biometric fingerprint lock. There is one door to the server room, which is secured by a standard lock and key.

The following individuals have a key to the server room: UCPD IS Manager, Lieutenant of the Investigations Unit, and two General Services IT staff who help support the RMS server. In order for the General Services IT staff to access the server room, they must check-in at the front lobby on the first floor and then be escorted by the UCPD IS Manager. If the UCPD IS Manager is not there (during off-hour times), these individuals must still check-in at the front lobby and obtain approval for access by the Watch Commander on duty.

There is also a backup key maintained in a key cabinet in the UCPD Command Center, on the first floor. Access to the UCPD Command Center is restricted by a biometric fingerprint lock. There is no security camera specific to the server room; however, all entrances to the UCPD building have security cameras.

There were no significant control weaknesses noted in this area.

1. Access to Paper Records

A&AS staff toured the office area where paper records are maintained to determine if access to paper records are secured and restricted to authorized personnel. Paper records are stored in locked file cabinets located in the Records Unit area, which only Records Unit staff have access to.

There were no significant control weaknesses noted in this area.

Availability of Records

The availability of records through RMS is critical to UCPD management. Plans, agreements, and practices to ensure the availability and timely recovery of RMS in the event of a disaster or disruption in business continuity were reviewed and discussed with UCPD management. The following were noted:

1. RMS Disaster Recovery Plan and Backups

Discussions were held with UCPD management to determine if there is a disaster recovery plan for RMS, noting that a business impact analysis has not been performed and recovery time objectives have not been defined.

Also, determined if backups of RMS are performed regularly, rotated off-site, and test restores are performed by confirming with UCLA Facilities Management IS (FMIS) department, who is responsible for backing up RMS. Based on discussions with FMIS, the following were noted: RMS is backed up daily, test restores are performed, and there have not been any issues with backups. RMS is backed up to two different storage appliances; one is located in the Facilities Management building, and the other is located in Transportation Services. However, both storage appliances are located on campus.  In the event of a major campus-wide disaster, backups at both locations may be destroyed.

Recommendation: UCPD management should perform a business impact analysis and identify how timely RMS would need to be recovered in the event of a disaster, and establish a plan that will meet their recovery time objectives. As part of their overall disaster recovery planning efforts, management should also assess if backups should be stored at a more distant location away from campus.

Response: Concur. The department will perform a business impact analysis and identify how RMS would need to be recovered in the event of a disaster, and establish a plan. This analysis will be completed by December 31, 2018.

1. RMS Support Agreement

A&AS verified that UCPD has a formal agreement with the software vendor, Superion, for support of RMS by obtaining and reviewing a copy of the agreement. The support agreement includes agreed upon response times, based on the criticality of reported system issues.

There were no significant control weaknesses noted in this area.

1. Server Room Environmental Controls

Environmental controls for the RMS server room were reviewed to determine that they are adequate and help ensure proper functioning of the RMS. A tour of the server room was conducted with the UCPD IS Manager, noting that the room is equipped with the following environmental controls: air conditioning, uninterruptible power supplies, and a fire sprinkler system.

There were no significant control weaknesses noted in this area.

Release of Records

UCPD records are released to individuals or agencies, to the general public to alert them of crimes, or printed for internal purposes. Records are only to be released to parties that have a right to know and a need to know. Crime alerts to the public should not include restricted information, such as juvenile or sexual assault conviction identities. The purpose and need for printing or releasing records must be documented. Review indicated the following:

1. Incident Reports - Releases to Individuals or Agencies

The Records Unit is responsible for ensuring that UCPD records are released appropriately by determining whether the party requesting a record has the right to know and the need to know. Requests can be made by individuals or authorized agencies, such as insurance agencies. The party requesting a record must submit a hard-copy form or other written document to explain the purpose of the request. Records Unit staff then determines the validity of the request. If approved, the party pays a fee to UCPD. The fee amount is dependent on the type of record requested (traffic collision, arrest report, etc.). Once payment is made, a copy of the requested report is printed, stamped, and released. The request form or other request document is scanned, uploaded into RMS, and attached to the report as a supplemental document.

From the same judgmental sample of ten incident reports that were reviewed for accuracy, completeness, and timeliness, with the assistance of the Records Manager, A&AS staff identified all the instances that each incident report was printed and/or released and verified if they were appropriate and properly documented. There were ten instances when an incident report was printed and/or released, including two that were released to outside entities, and eight that were printed for internal purposes.  For the release of police reports to outside entities, an "Application for Release of Information" form must be completed and signed by the requestor.  There was a completed and signed form for one of the releases; however, not for the second release.  Although there was not a completed form, the incident was for driving under the influence and the report was released to the Department of Motor Vehicles, which appears appropriate because the report was released to an authorized entity, based on the incident.

There were no significant control weaknesses noted in this area.

1. Application for Release of Information Form

The "Application for Release of Information" form could be improved by requiring some additional information. The current form requires limited information about the report being requested, such as the date and time and location of the incident, the name and signature of the requestor, party of interest, and date of request.

Recommendation: The Records Unit should consider revising the "Application for Release of Information" form to require that the following additional information be documented: person authorizing the release, person releasing the report, date report was released, if a fee was collected or waived, and if a request is denied, the reason why.

Response: Concur. The department will consider revising the "Application for Release of Information" form to require that these additional information be documented. This assessment will be completed by August 1, 2018.

1. Police Reports - Reason for Printing Reports

When police reports are printed from RMS for internal purposes or released to outside entities, the system and internal department policies require the reason the report needed to be printed, and who received the report must be documented. For nine of the ten instances when a police report was printed or released, the reason for printing and releasing the reports and who received the reports were clearly documented. However, there was one instance when a detective could have provided a clearer reason as to why a police report needed to be printed.

Recommendation: UCPD management should remind staff that the reason for printing and releasing police reports should be clearly documented.

Response: Concur. The department will remind staffs to document the reason for printing and releasing police reports.

1. Crime Alerts - Releases to the Public

Crime alerts are posted on the UCPD’s website. A judgmental sample of ten crime alerts posted during fiscal year 2017-18 were reviewed to verify that inappropriate information such as juvenile or sexual assault conviction identities are not disclosed.

There were no significant control weaknesses noted in this area.

Records Retention

UCPD’s records retention schedule was reviewed and discussed with UCPD management to determine if it is in accordance with current laws, regulations, and University policies.

Records Retention Schedule

A records retention schedule was created for UCPD back in 2007; however, the schedule has not been reviewed and revised since it was created. The Lieutenant of the Investigations Unit indicated the retention schedule for some of the records are not accurate.  For example, the retention period for all crime reports is not seven years as recommended in the schedule, as there are some crimes for which evidence and related police reports need to be retained for up to 20 years.  Based on discussions with the UCPD Records Manager they have not purged any records.

Recommendation: UCPD management should update their records retention schedule and ensure that their records are retained or disposed in accordance with current laws, regulations, and University policies.

Response: Concur. The department will update the records retention schedule to ensure that our records are retained or disposed in accordance with current law, regulation, and University policies. This will be completed by December 31, 2018.

180322-2
REP