Memorandum

CITY OF DALLAS
(Report No. A18-011)

DATE: June 22, 2018

TO: Honorable Mayor and Members of the City Council

SUBJECT: Audit of the Dallas Police Department's Records Management System[1]

For the audit period, (June 1, 2014 through June 30, 2017), the Dallas Police Department (DPD) had adequate internal controls to ensure that all crime related data were processed efficiently and effectively. The DPD reported complete, correctly classified, and accurate counts of serious crime incidents[2] and arrests[3] to the Texas Department of Public Safety (TX DPS). As a result, the citizens of Dallas, the TX DPS, and the United States Federal Bureau of Investigation (FBI) can rely on the crime statistics reported by DPD. (**Note**: The TX DPS reports this DPD

Background

The Records Management System (RMS) is a software application used to collect, store, and provide access to law enforcement information gathered during the investigation of a crime incident.

The RMS information includes crime incident reports with the type of the offense, victims, suspects, report narrative, and investigative steps taken by the Dallas Police Department (DPD). It also shows whether a case was solved, and the suspect was arrested. The RMS information is used for investigations, preparing criminal cases for prosecution, tracking criminal data, and for producing statistical crime reports, including the reports to the Texas Department of Public Safety (TX DPS).

Source: RMS Training Manual

[1] This audit was conducted under the authority of the City Charter, Chapter IX, Section 3 and in accordance with the Fiscal Year 2015 Audit Plan approved by the City Council. The original audit objective was to determine whether the City of Dallas' (City) goals for implementing the Records Management System (RMS) achieved anticipated results (specifically cost, project schedule, functions implemented, and shadow systems eliminated) and whether the RMS includes appropriate controls. The audit objective was revised to determine if the RMS has adequate internal controls to ensure that all crime related data are processed efficiently and effectively. The audit scope included RMS crime incidents reported from June 1, 2014 to June 30, 2017; however, certain other matters, procedures, and transactions occurring outside that period may have been reviewed to understand and verify information related to the audit period. This audit was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based upon our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. To achieve the audit objective, we interviewed the Dallas Police Department (DPD) personnel; reviewed DPD policies and procedures, the Texas Family Code, the Texas Penal Code, Administrative Directive 2-24, *Computer Security*, *Standards for Internal Control in the Federal Government* established by the United States Government Accountability Office in September 2014 (Green Book), the Criminal Justice Information System (CJIS) Security Policy, and the City's Enterprise Information Security Standard (EISS); tested representative random and judgmental samples of transactions and performed various analyses.

[2] The count of crime incidents did not include a verification of the number of victims for crimes against persons, burglary, larceny, and robbery attempts, and the number of stolen motor vehicles.

[3] For TX DPS reporting purposes criminal homicide, rape, robbery, aggravated assault, burglary, larceny-theft, motor vehicle theft (Part I offenses) plus the offenses of simple assault and manslaughter by negligence are reported on the *RETURN A – MONTHLY RETURN OF OFFENSES KNOWN TO THE POLICE*. The DPD also reports arrests monthly on the following forms: *AGE, SEX, & RACE OF PERSONS ARRESTED – Under 18 and AGE, SEX, & RACE OF PERSONS ARRESTED - Over 18.*

information to the FBI's Uniform Crime Reporting (UCR) Program)[4].

The DPD's internal controls related to the Records Management System (RMS), however, are not sufficient to:

- Prevent and detect unauthorized deletions or alterations of RMS data
- Ensure only users who need access to RMS to perform their job responsibilities have access

The issues and associated recommendations resulting from this audit are discussed in more detail on the following pages. In addition, please see Attachment I - Background for additional information related to the audit.

DPD Reported Complete, Correctly Classified, and Accurate Counts of Serious Crime Incidents and Arrests

Based on our analysis it appears that the DPD submitted complete, correctly classified, and accurate counts of serious crime incidents and arrests to the TX DPS for the audit period. As a result, the citizens of Dallas, the TX DPS, and the FBI can rely on the crime statistics reported by DPD. Specifically, from January 1, 2015[5] to June 30, 2017, DPD correctly classified and reported:

- 99.9 percent of all serious crime incidents
- 99.9 percent of all arrests

UCR Reports to TX DPS

DPD submits several monthly reports to the Texas Department of Public Safety (TX DPS). The primary report is the *RETURN A – MONTHLY RETURN OF OFFENSES KNOWN TO THE POLICE* that shows counts of the more serious offenses known to DPD.

Two reports, the *AGE, SEX, & RACE OF PERSONS ARRESTED – Under 18* and the *AGE, SEX, & RACE OF PERSONS ARRESTED - Over 18* track arrests and information about arrested persons. Other reports provide information about stolen property, arson, law enforcement officers that were killed or assaulted, juvenile offenders, and university campus crime statistics.

Source: RMS Training Manual

In addition, based upon tests of crime incident report narratives in RMS from June 1, 2014 through June 30, 2017, DPD accurately classified crime incidents as follows:

- 100 percent of crime incidents required to be reported to TX DPS
- 93.3 percent that are not required to be reported to TX DPS

[4] The Uniform Crime Reporting (UCR) Program was conceived in 1929 by the International Association of Chiefs of Police to meet the need for reliable uniform crime statistics for the nation. In 1930, the FBI was tasked with collecting, publishing, and archiving those statistics.

[5] The DPD did not provide the monthly diagnostic reports from June 1, 2014 through January 1, 2015; therefore, these months were excluded for audit testing purposes.

To help ensure the accuracy of statistical reporting, DPD has instituted multi-stage error checks. For example, a Staff Review Team reads all crime reports composed by DPD officers in the field and checks all required fields for accuracy. Inaccurately completed reports are sent back to DPD officers for corrections.

From June 1, 2014 (RMS Go-Live date) to June 30, 2017, DPD officers and the Staff Review Team achieved a high level of accuracy in filling out crime reports, which is reflected by the fact that 98 percent of all reports were approved by Staff Review upon first submission. In addition, a UCR Group reviews the accuracy of all Part I crime reports and a sample of Part II reports and then runs a variety of error-checking queries to identify and correct data entry errors.

Standards for Internal Control in the Federal Government by the Comptroller General of the United States (Green Book) requires management to meet the information processing objectives of data completeness, accuracy, and validity. In addition, the FBI and the TX DPS require UCR Program participants to produce reliable crime statistics.

Internal Controls are Inadequate to Prevent and Detect Unauthorized Deletions or Alterations of RMS Data

The DPD does not have internal controls to prevent and detect unauthorized deletions or alterations of RMS data. As a result, there is an increased risk that the crime incidents and the associated details could be altered, deleted, or fraudulently manipulated without detection by DPD. Specifically, DPD does not have formal policies and procedures (written, approved, and dated) that prescribe how to:

- Request and authorize the legitimate alteration and expungement[6] of data from RMS
- Monitor the data completeness, accuracy, and validity of RMS crime data
- Regularly review crime data audit logs for indications of inappropriate or unusual activity
- Identify and investigate suspicious activity or suspected unauthorized data alterations and take appropriate corrective and disciplinary actions

From June 1, 2014 to June 30, 2017, three hundred and eighty-four crime reports were deleted from the RMS. While some of these crime reports may have been legitimately expunged in response to court orders of expunction, DPD cannot ascertain which crime reports were legally expunged and which crime reports were unintentionally or willfully

[6] According to the Texas Code of Criminal Procedure, Chapter 55. Expunction of Criminal Records, a person who has been acquitted of a felony or misdemeanor is entitled to have all records and files relating to the arrest expunged by petitioning for and obtaining a court order of expunction which requires the DPD to obliterate all portions of the record or file that identify the petitioner.

deleted from RMS without authorization because audit logs[7] related to these crime reports were also deleted.

In addition, DPD cannot prevent unauthorized deletions or alterations of RMS data because of several internal control weaknesses related to user access to RMS data, such as segregation of duties and assigning least privileges discussed in more detail in the next report issue.

The Green Book requires management to meet the information processing objectives of data completeness, accuracy, and validity. In addition, the TX DPS defines the objective of the UCR program as: "to produce reliable crime statistics."

Both the City's Administrative Directive 2-24, *Computer Security* (AD 2-24) and the Criminal Justice Information System (CJIS) Security Policy have a number of requirements for the DPD and the Department of Communication and Information Services (CIS). See Attachment II for additional details on these requirements.

Internal Controls over User Access to RMS Data are Inadequate

The DPD does not have adequate internal controls over user access to RMS data. As a result, DPD cannot prevent unauthorized users from accessing and potentially compromising RMS data without detection. For example, DPD does not have a matrix of user access privileges based on the principles of segregation of duties and assigning least privileges (see textbox). A review of user access privileges in RMS shows the following access control weaknesses:

Internal Controls over User Access

Segregation of Duties

The functions of authorization, recording, custody of records, and reconciliation or audit of records should be segregated among users.

Assigning Least Privileges

Giving each authorized user account access to only those privileges which are essential to perform the user's intended duties.

Source: National Institute of Standards and Technology. U.S. Department of Commerce. Publication 800-53 Revision 4. Security and Privacy Controls for Federal Information Systems and Organizations.

- Users assigned to the "Records" group, who have the custody of RMS records, also have the ability to alter or even delete the underlying RMS data

- Uniform Crime Reporting (UCR) Team personnel who are tasked with reconciling RMS data and producing statistical crime reports for the TX DPS, also have the ability to alter the underlying RMS data. Users assigned to the Crime Analysis Unit who are tasked with producing statistical crime reports for the DPD command staff also have the ability to alter the underlying RMS data.

[7] An audit log is a document that records an event in an information (IT) technology system. An event, in the computing context, is any identifiable occurrence that has significance for system hardware or software.

- Sixteen users have unrestricted ability to delete crime reports without authorization

- All DPD investigators have the ability to alter the details of all crime reports in RMS even if they are not assigned to investigate them

In addition, since the implementation of RMS in June 2014, CIS has not performed a required annual review of RMS user access privileges. The Office of the City Auditor's review of user access privileges in RMS showed:

- Over 900 of 4,681, or approximately 21 percent of the active user accounts are assigned to individuals who are no longer employed by the City of Dallas

- At least 19 active generic accounts that do not identify a specific user; for example, a user named "password.admin1" with a "password.admin1" user ID

- Temporary and outdated user groups that are no longer used; for example, a "dpdtrainer" group was created to provide mass RMS training to DPD personnel during RMS implementation

- Users with the same job duties have different user access privileges. For example, as shown in Table I below, DPD Patrol Supervisors have different access privileges depending upon their location within the City.

Table I

Illustration of Different Access Privileges for DPD Patrol Supervisors

User Group	User Group Definition	Number of Tables with WRITE Access	Number of Security Features Available to Users
NE_PTROL_SUP	Northeast Patrol Division Supervisors	1	104
NW_PTROL_SUP	Northwest Patrol Division Supervisors	1	105
SC_PTROL_SUP	South Central Patrol Division Supervisors	2	104
SE_PTROL_SUP	Southeast Patrol Division Supervisors	1	136
SW_PTROL_SUP	Southwest Patrol Division Supervisors	0	135
CBD_PTRL_SUP	Central Business District Patrol Division Supervisors	212	103

Source: RMS

According to the Green Book, management limits access to resources and records to authorized individuals and assigns and maintains accountability for their custody and use. Management may periodically compare resources with the recorded accountability to help reduce the risk of errors, fraud, misuse, or unauthorized alteration.

The City's Enterprise Information Security Standard (EISS) requires DPD to annually assess user access, appropriate roles, staff employment status, and logon activities for each information system, asset, and user account. See Attachment II for additional details on EISS requirements.

We recommend the Chief of Police:

I. Implements formal policies and procedures to ensure:

- Any legitimate alteration and expungement of data from RMS is formally requested, authorized, and documented by DPD management
- Crime data audit logs are preserved and regularly reviewed for indications of inappropriate or unusual activity

II. Develops a matrix of user access privileges in RMS that would ensure segregation of incompatible duties and the assignment of least privileges to each user that are essential to perform the user's assigned duties

III. Uses the matrix of user access privileges to re-assign user access in RMS based on the principles of segregation of incompatible duties and the assignment of least privileges to each user that are essential to perform the user's intended duties

IV. Implements formal policies and procedures to perform an annual comparison of user access privileges in RMS to the matrix of user access privileges.

V. Deactivates RMS user accounts of users who are no longer employed by the City

VI. Ensures DPD complies with the City's EISS, specifically:

- Assigns a unique personal user account to every RMS user
- Limits temporary access to an elevated privilege, such as an administrator, to seven days
- Disables and locks RMS users accounts when the individual has not accessed RMS for any consecutive 90-day period

- Deactivates/disables vendor accounts if the accounts have not been used in any consecutive 90-day period

- Revokes user access to RMS immediately upon termination of employment

- Logs the activities of all elevated accounts and reviews the logs regularly to ensure that inappropriate activities are identified early and resolved

We recommend the Director of CIS:

VII. Performs security reviews and security assessments of RMS in accordance with the EISS

Please see Attachment III for management's response to the recommendations made in this report.

We would like to acknowledge management's cooperation during this audit. If you have any questions or need additional information, please contact me at 214-670-3222 or Carol Smith, First Assistant City Auditor, at 214-670-4517.

Sincerely,

Craig D. Kinton
City Auditor

Attachments

C: T. C. Broadnax - City Manager
Kimberly B. Tolbert - Chief of Staff
Jon Fortune - Assistant City Manager
Jo M. (Jody) Puckett, P.E - Interim Assistant City Manager
U. Renee Hall - Chief of Police
William Finch, Director – CIS

ATTACHMENT I

Background

Records Management System

The Dallas Police Department (DPD) uses a Records Management System (RMS) to collect and store law enforcement data used for crime investigations and for calculating crime statistics. The RMS allows DPD to capture and track operational data such as crime incidents, suspects, arrests, witnesses, victims, locations, descriptions of vehicles, etc.

Most crime reports are initiated in the field by DPD patrol officers from a workstation or patrol vehicle by accessing the Field Based Reporting (FBR) application to enter the appropriate data to create crime reports. These crime reports are then forwarded to the Staff Review Team for approval before they are sent to the RMS.

Staff Review Team

The Staff Review Team provides crime report review and approval 24 hours a day by operating three eight-hour shifts of six people each shift. The Staff Review Team reads the crime reports and checks all required fields for accuracy. Then, the Staff Review Team either approves the crime reports and forwards them to DPD investigators for further action or rejects the crime reports and sends them back to the patrol officers for corrections. Each person on the Staff Review Team reviews between 50 to 80 crime reports per eight-hour shift.

Uniform Crime Reporting

The DPD also uses the RMS to generate monthly Uniform Crime Reporting (UCR) statistical reports for the Texas Department of Public Safety (TX DPS). The UCR reports contain data relating to criminal offenses and arrests.

To ensure the accuracy of the reports, DPD has created a UCR Team consisting of ten individuals. The UCR Team also reviews crime reports and arrests for errors by reading all Part I crime reports except Arson and a small selection of Part II crime reports entered into the RMS system.[8]

In addition, the UCR Team runs several error-checking queries to detect data entry errors that would prevent a criminal case from being counted for statistical reporting. The UCR Team members correct the errors themselves or by contacting the individuals who originally wrote the crime reports.

[8] See Table II for Part I and Part II offenses in RMS.

Uniform Crime Reporting (continued…)

The UCR reports are based on a "Hierarchy Rule", which classifies the crimes according to how serious they are, with criminal homicide being the highest in the hierarchy and arson being the lowest for Part I offenses. The "Hierarchy Rule" requires DPD to report each single-offense incident, however, in multiple-offense situations, DPD must identify and report the offense that is highest on the hierarchy list and omit the other offense(s) from the count.

The "Hierarchy Rule" applies only to crime reporting and does not affect the number of charges for which the defendant may be prosecuted in the courts. The offenses of justifiable homicide, motor vehicle theft, and arson are exceptions to the "Hierarchy Rule".

During the audit period, DPD recorded a total of 762,054 crime incidents in the RMS, of which 170,644 were the more serious Part I offenses. See Table II for the breakdown of all offenses in RMS:

Table II

RMS Offenses by Type During the Audit Period.

Offense	Offense Type	Total
AGGRAVATED ASSAULT	PART I	11,658
AUTO THEFT	PART I	24,570
BURGLARY	PART I	34,528
MURDER	PART I	441
RAPE	PART I	2,679
ROBBERY	PART I	13,645
THEFT	PART I	82,264
ARSON	PART I	859
PART I Subtotal		**170,644**

Note: Part II Offenses continued on next page

RMS Offenses by Type During the Audit Period.

Offense	Offense Type	Total
ANIMAL BITE	PART II	1,157
ASSAULT	PART II	60,156
CHILD (OFFENSES AGAINST)	PART II	4,433
CRIMINAL MISCHIEF/VANDALISM	PART II	45,052
DISORDERLY CONDUCT	PART II	7,825
DRUNK & DISORDERLY	PART II	12,404
DWI	PART II	2,221
EMBEZZLEMENT	PART II	2,154
FAIL TO ID	PART II	865
FORGERY & COUNTERFEIT	PART II	2,950
FRAUD	PART II	4,723
GAMBLING	PART II	24
INTOXICATION MANSLAUGHTER	PART II	22
LIQUOR	PART II	154
LOST PROPERTY	PART II	527
MOTOR VEHICLE ACCIDENT	PART II	25,816
NARCOTICS/DRUGS	PART II	4,252
OTHER OFFENSES	PART II	14,573
PROSTITUTION	PART II	260
RUNAWAY	PART II	8,595
SEX OFFENSES/INDECENT CONDUCT	PART II	1,523
TRAFFIC	PART II	398
WEAPONS	PART II	872
PART II Subtotal		**200,956**

Note: Other Offenses continued on next page

RMS Offenses by Type During the Audit Period.

Offense	Offense Type	Total
NO UCR REPORTABLE OFFENSE	OTHER	606
ACCIDENTAL INJURY	OTHER	4,828
AIRPLANE	OTHER	1
ALARM INCIDENT	OTHER	88,083
ATTEMPTED SUICIDE	OTHER	689
FIREARMS ACCIDENT	OTHER	326
FOUND PROPERTY	OTHER	30,259
HOME ACCIDENT	OTHER	2,580
LOST PROPERTY	OTHER	3,463
MISCELLANEOUS	OTHER	157,513
MISSING PERSON	OTHER	798
NO UCR REPORTABLE OFFENSE	OTHER	65,508
OCCUPATIONAL ACCIDENT	OTHER	168
PRELIMINARY INVESTIGATION	OTHER	28,171
SEIZED PROPERTY	OTHER	2,619
SUDDEN DEATH	OTHER	4,170
SUICIDE	OTHER	294
TRAFFIC FATALITY	OTHER	362
BLANK	OTHER	16
OTHER Subtotal		**390,454**
Grand Total		**762,054**

Source: RMS

In 2018, DPD began transitioning to a National Incident Based Reporting System (NIBRS), which is an incident-based reporting system for crimes known to the police. Unlike the UCR's hierarchy-based reporting, in NIBRS each crime incident is counted, and a variety of data are collected about each incident. These data include the nature and types of specific offenses in the incident, characteristics of the victim(s) and offender(s), types and value of property stolen and recovered, and characteristics of persons arrested in connection with a crime incident.

ATTACHMENT II

Relevant Information Security Requirements

Administrative Directive 2-24, *Computer Security*

Administrative Directive 2-24, Computer Security (AD 2-24) requires City of Dallas (City) departments to:

- Protect the City's information technology (IT) assets, resources, and data from unauthorized access, use, disclosure, disruption, modification, or destruction
- Establish IT security programs, including assignment of roles and responsibilities
- Restrict access to the City's information systems and assets with various access controls and mechanisms
- Prohibit unauthorized access to, or unauthorized use of, information systems and assets without formal approval
- Restrict access to information systems to only those with the need to access such systems
- Periodically review and classify RMS data to enable the Department of Communication and Information Systems (CIS) to implement appropriate security controls for such data

.

The AD 2-24 also requires CIS and the Dallas Police Department (DPD) to implement continuous monitoring of systems to control and prevent unauthorized access to the City's information systems and assets.

City of Dallas Enterprise Information Security Standard

The City of Dallas Enterprise Information Security Standard (EISS) requires DPD to ensure:

- Existing security controls are appropriate, effective, and aligned with the accepted risks to the information systems and assets being assessed
- Every user account has least privileges assigned to it by default by administrators
- Every user accessing the City's information systems and networks has a unique personal user account
- Temporary access to the elevated privilege is limited to a maximum period of seven days

- If the City employee account is not used at least once in any consecutive 90-day period, said account will be "locked/disabled"

- If a vendor's account is not used at least once in any consecutive 90 days, said account will be deleted

- User access to the public safety systems Criminal Justice Information Systems (CJIS) is revoked immediately upon separation in employment with the City

The activities of all elevated accounts or their equivalents are logged by the host operating system logging facilities where available and the logs are reviewed regularly by support staff to ensure that inappropriate activities are identified early and resolved.

In addition, the EISS requires CIS to perform annual security reviews and security assessments of RMS.

Criminal Justice Information Services Security Policy

The CJIS Security Policy requirements are to:

- Establish procedures to protect information from unauthorized disclosure, alteration, or misuse

- Generate audit records for significant events relevant to the security of the information system

- Produce audit records containing sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events

- Review and analyze information system audit records for indications of inappropriate or unusual activity, investigate suspicious activity or suspected violations to report findings to appropriate officials and to take necessary actions

- Retain audit records for at least one year

- Identify authorized users of the information system and specify access rights and privileges

- Control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) in the information system

- Implement least privilege based on specific duties, operations, or information systems as necessary to mitigate risk to criminal justice information

ATTACHMENT III

Management's Response

Memorandum

RECEIVED

JUN 20 2018

City Auditor's Office

CITY OF DALLAS

DATE: May 18, 2018

TO: Craig D. Kinton, City Auditor

SUBJECT: Response to Audit Report:
Audit of the Dallas Police Department's Records Management System

Our responses to the audit report recommendations are as follows:

Recommendation I

We recommend the Chief of Police implements formal policies and procedures to ensure:

- Any legitimate alteration and expungement of data from RMS is formally requested, authorized, and documented by DPD management
- Crime data audit logs are preserved, and regularly reviewed for indications of inappropriate or unusual activity

Management Response/Corrective Action Plan

Agree ☒ Disagree ☐

Per post-audit discussions, DPD is not allowed to keep any information concerning the expungement order, including the order itself. Per Audit Recommendations, DPD will implement a policy in which the number of records to be deleted are assigned daily, are documented, and will include the number of deletions actually performed each day. This document will be signed by both the employee performing the deletion as well as their Supervisor. They will be titled deletions due to the law requiring no records of any expungements. DPD will compare the total number of data deletions to the number of authorized data deletions as part of the annual review of user access privileges in RMS. DPD will investigate all instances of unauthorized data deletions in RMS.

Implementation Date
11/30/18

Responsible Manager
Records/ Legal Services Lieutenant

"Our Product is Service"
Empathy | Ethics | Excellence | Equity

Page 1 of 6

Recommendation II

We recommend the Chief of Police develops a matrix of user access privileges in RMS that would ensure segregation of incompatible duties and the assignment of least privileges to each user that are essential to perform the user's assigned duties.

Management Response/Corrective Action Plan

Agree ☒ Disagree ☐

Per Audit Recommendation, DPD will create a matrix of user access privileges in RMS to ensure that segregation of incompatible duties are identified and any incompatible duties are modified to give each user the least privileges necessary to perform their assigned duties.

Implementation Date
11/30/18

Responsible Manager
Operational Technology Lieutenant

Recommendation III

We recommend the Chief of Police uses the matrix of user access privileges to re-assign user access in RMS based on the principles of segregation of incompatible duties and the assignment of least privileges to each user that are essential to perform the user's intended duties.

Management Response/Corrective Action Plan

Agree ☒ Disagree ☐

Per Audit Recommendation, each user's access will be modified to ensure that they have the least amount of privileges necessary to perform the user's intended duties.

Implementation Date
11/30/18

Responsible Manager
Operational Technology Lieutenant

Recommendation IV

We recommend the Chief of Police implements formal policies and procedures to perform an annual comparison of user access privileges in RMS to the matrix of user access privileges.

Management Response/Corrective Action Plan

Agree ☒ Disagree ☐

Per the Audit Recommendation, a formal process will be created and implemented to perform an annual review/comparison of user access privileges in RMS to ensure that the privileges are in alignment with the matrix that will be created as recommended in Recommendation II. This audit will be conducted by the RMS team and will be verified by the sergeant over the RMS team.

Implementation Date
11/30/18

Responsible Manager
Operational Technology Lieutenant

Recommendation V

We recommend the Chief of Police deactivates RMS user accounts for users who are no longer employed by the City.

Management Response/Corrective Action Plan

Agree ☒ Disagree ☐

Per the Audit Recommendation, the RMS application will be linked to the City's Active Directory services to ensure that the accounts for users who are no longer employed by the City are deactivated at the same time their network accounts are deactivated by CIS' Security team. DPD has already implemented a secondary process to ensure they are removed during the exit process.

Implementation Date
11/30/18

Responsible Manager
Operational Technology Lieutenant

Recommendation VI

We recommend the Chief of Police ensures DPD complies with the City's EISS, specifically:

- Assigns a unique personal user account to every RMS user
- Limits temporary access to an elevated privilege, such as an administrator, to seven days
- Disables and locks RMS user accounts when the individual has not accessed RMS for any consecutive 90-day period
- Deactivates/disables vendor accounts if the accounts have not been used in any consecutive 90-day period
- Revokes user access to RMS immediately upon termination of employment
- Logs the activities of all elevated accounts and reviews the logs regularly to ensure that inappropriate activities are identified early and resolved

Management Response/Corrective Action Plan

Agree ☒ Disagree ☐

Per the Audit Recommendation, the RMS application will be linked to the City's Active Directory services to ensure that the accounts for users who fall into the various categories above (no longer employed, deactivation of vendor accounts in 90 days, etc.) are deactivated at the same time their network accounts are deactivated by CIS' Security team.

Implementation Date
11/30/18

Responsible Manager
CIS Security Manager

J. Renee Hall, Chief of Police 6-20-2018
Assistant City Manager

Jon Fortune
Assistant City Manager

"Our Product is Service"
Empathy | Ethics | Excellence | Equity

Memorandum

RECEIVED

JUN 5 2018

City Auditor's Office

CITY OF DALLAS

DATE: June 5, 2018

TO: Craig D. Kinton, City Auditor

SUBJECT: Response to Audit Report:
Audit of the Dallas Police Department's Records Management System

Our responses to the audit report recommendations are as follows:

Recommendation VII

We recommend the Director of CIS performs security reviews and security assessments of RMS in accordance with the EISS.

Management Response/Corrective Action Plan

Agree ☒ Disagree ☐

CIS will perform security reviews and security assessments of RMS in accordance with the EISS.

Implementation Date
Develop requirements – October 31, 2018
Refine schedule – December 31, 2018
Demonstration of sustainability – January 1, 2019 – December 31, 2020

Responsible Manager
CIS Compliance Manager

Sincerely,

William Finch
Director of CIS

Jo M. (Jody) Puckett, P.E.
Interim Assistant City Manager

C: T.C. Broadnax, City Manager
Kimberly B. Tolbert, Chief of Staff

"Our Product is Service"
Empathy | Ethics | Excellence | Equity

Page 1 of 1