The Auditor of the City and County of Denver is independently elected by the citizens of Denver. He is responsible for examining and evaluating the operations of City agencies for the purpose of ensuring the proper and efficient use of City resources and providing other audit services and information to City Council, the Mayor and the public to improve all aspects of Denver’s government. He also chairs the City’s Audit Committee.

The Audit Committee is chaired by the Auditor and consists of seven members. The Audit Committee assists the Auditor in his oversight responsibilities of the integrity of the City’s finances and operations, including the integrity of the City’s financial statements. The Audit Committee is structured in a manner that ensures the independent oversight of City operations, thereby enhancing citizen confidence and avoiding any appearance of a conflict of interest.

Audit Committee

Dennis Gallagher, Chair
Maurice Goodgaine
Leslie Mitchell
Rudolfo Payan

Robert Bishop
Jeffrey Hart
Timothy O’Brien, Vice-Chair

Audit Staff

Audrey Donovan, Deputy Director, CIA, CRMA
Stephen E. Coury, IT Audit Supervisor, CISA
Roman Bukhtiyar, Senior IT Auditor, CISA
Ketki Dhamanwala, Senior IT Auditor, CIA, CISA

You can obtain copies of this report by contacting us at:

Office of the Auditor
201 West Colfax Avenue, Department 705 • Denver CO, 80202
(720) 913-5000 • Fax (720) 913-5247

Or download and view an electronic copy by visiting our website at:

www.denvergov.org/auditor
Mr. Alex Martinez, Manager of Safety
Mr. Michael Wright, Chief Information Officer, Technology Services
City and County of Denver

Dear Messrs. Martinez and Wright,

Attached is the Auditor’s Office Audit Services Division’s report reviewing the Police Records Management System Information Technology General Controls. The purpose and overall objective of the audit was to examine and assess the IT general controls related to the Police Department’s Records Management System to ensure that they provide a sound foundation to support the system’s proper operation and security.

“Don’t put all your eggs in one basket.” This quote from Don Quixote is commonly understood to mean that one should not overly concentrate important items in one place. This can certainly be applied to computer system backups. It is best practice to save your backup files in a safe place far away from your main computer systems. That way, if there is ever a problem with your data center, you can retrieve your data and start anew somewhere else. The City has not followed this sage advice with respect to the critical systems supporting our Safety Departments. Backup files are stored just a few feet away from their primary systems within the same data center. I cannot emphasize enough the seriousness of this shortcoming in our backup strategy. Should a disaster ever befall the data center, such as a fire, we could risk total loss of our electronic records for all the Police, Fire, and Sheriff Departments. The lack of a written disaster recovery plan and the failure to perform tests to demonstrate recovery capability for the Police Records Management System exacerbates this issue.

In addition, our auditors found that the daily tasks performed to backup important systems, such as the Police Department’s Records Management System, had an unusual number of failures. Closer examination determined that the backup tasks were failing because the servers were running out of disk space. Further research determined that the disk space shortage was not limited to the Police Department, but affected all systems housed within the same data center, such as the Jail Management System, the Office of Systems Integration, mug shots, as well as all the High Activity Location Observation (HALO) video recordings, amongst others.

Technology Services personnel, although aware of disk space shortages, were caught off guard when we notified them that backup tasks were failing, in some cases, for up to eleven straight days. Had there been a need to recover from a backup during that period, several days worth of data may have been lost, adversely affecting current police operations.

As I alerted you and the leaders of the City’s Safety Departments on October 4, 2012, these are serious shortcomings that require immediate remediation. I am encouraged, however, by the responses that we have received from Technology Services indicating that solutions for both
The offsite storage of backup files and the storage capacity to make backups are in the works. As Shakespeare said in Coriolanus, “Action is eloquence.”

This audit also highlights several other important issues, such as user administration, antivirus and system patching, data center security, and change management. Please see the attached report for more details. You will find a copy of my alert letter and the response from Technology Services in Appendices A and B, respectively.

If you have any questions, please call Kip Memmott, Director of Audit Services, at 720-913-5000.

Sincerely,

Dennis J. Gallagher
Auditor

DJG/sec

cc: Honorable Michael Hancock, Mayor
    Honorable Members of City Council
    Members of Audit Committee
    Ms. Cary Kennedy, Deputy Mayor, Chief Financial Officer
    Ms. Janice Sinden, Chief of Staff
    Ms. Stephanie O’Malley, Deputy Chief of Staff
    Ms. Beth Machann, Controller
    Mr. Doug Friednash, City Attorney
    Ms. Janna Bergquist, City Council Executive Staff Director
    Mr. L. Michael Henry, Staff Director, Board of Ethics
    Mr. Sean Curley, Co-Deputy Chief Information Officer
    Mr. Ethan Wain, Co-Deputy Chief Information Officer
AUDITOR’S REPORT

We have completed an audit of the Police Records Management System IT General Controls. The purpose and overall objective of the audit was to examine and assess the IT general controls related to the Police Department’s Records Management System (RMS) to ensure that they provide a sound foundation to support the system’s proper operation and security. Audit work focused on the controls over account provisioning, logical access, activity monitoring, system and antivirus update and patching, mobile device security, backup and recovery, service level performance, data center security, and change management. These controls were reviewed to varying degrees as applicable at the RMS application, Oracle database, and Linux server levels.

This performance audit is authorized pursuant to the City and County of Denver Charter, Article V, Part 2, Section 1, General Powers and Duties of Auditor, and 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 on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The audit found that Police, Fire, and Sheriff Department electronic records are at risk of total loss, should there be a data center disaster. The risk of total loss results from backup files not being stored off site, along with failures in creating backup files. The lack of a written disaster recovery plan and the failure to perform tests to demonstrate recovery capability for the Police Records Management System exacerbates this issue. Although the most significant risk identified in this audit relates to backup and recovery capability, there are several other important issues concerning, user administration, antivirus and system patching, data center security, and change management. Please see the Findings section of this report for more details.

We extend our appreciation to the Chief Information Officer in Technology Services and the Deputy Chief of Administration in the Police Department and the personnel who assisted and cooperated with us during the audit.

Audit Services Division

Kip Memmott, MA, CGAP, CRMA
Director of Audit Services
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>EXECUTIVE SUMMARY</td>
<td>1</td>
</tr>
<tr>
<td>INTRODUCTION &amp; BACKGROUND</td>
<td>3</td>
</tr>
<tr>
<td>What Is a Records Management System?</td>
<td>3</td>
</tr>
<tr>
<td>The Denver Police Department RMS</td>
<td>3</td>
</tr>
<tr>
<td>Criminal Justice Information Services Security Policy</td>
<td>4</td>
</tr>
<tr>
<td>Safety Data Center</td>
<td>4</td>
</tr>
<tr>
<td>What Are IT General Controls?</td>
<td>4</td>
</tr>
<tr>
<td>The Importance of Backups</td>
<td>4</td>
</tr>
<tr>
<td>SCOPE</td>
<td>6</td>
</tr>
<tr>
<td>OBJECTIVE</td>
<td>6</td>
</tr>
<tr>
<td>METHODOLOGY</td>
<td>6</td>
</tr>
<tr>
<td>FINDING 1</td>
<td>8</td>
</tr>
<tr>
<td>Police, Fire, and Sheriff Department Electronic Records Are At Risk of Total Loss Should There Be a Data Center Disaster</td>
<td>8</td>
</tr>
<tr>
<td>RECOMMENDATIONS</td>
<td>11</td>
</tr>
<tr>
<td>FINDING 2</td>
<td>12</td>
</tr>
<tr>
<td>User Administration Controls Do Not Ensure Timely Termination of Access or Adequate User Activity Monitoring</td>
<td>12</td>
</tr>
<tr>
<td>RECOMMENDATIONS</td>
<td>13</td>
</tr>
<tr>
<td>FINDING 3</td>
<td>13</td>
</tr>
<tr>
<td>System Software Patches and Antivirus Updates Are Not Monitored for Successful Installation and Sometimes Not Applied At All</td>
<td>13</td>
</tr>
<tr>
<td>RECOMMENDATIONS</td>
<td>14</td>
</tr>
</tbody>
</table>
# TABLE OF CONTENTS *(continued)*

<table>
<thead>
<tr>
<th>FINDING 4</th>
<th>15</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Safety Data Center Has No Automated Fire Suppression and Lacks Adequate Physical Access Controls</td>
<td>15</td>
</tr>
</tbody>
</table>

**RECOMMENDATIONS**

<table>
<thead>
<tr>
<th>FINDING 5</th>
<th>16</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minor Project Change Management Does Not Provide Adequate Segregation of Duties</td>
<td>16</td>
</tr>
</tbody>
</table>

**RECOMMENDATIONS**

<table>
<thead>
<tr>
<th>APPENDICES</th>
<th>17</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appendix A – Auditor’s Alert Letter</td>
<td>17</td>
</tr>
<tr>
<td>Appendix B – Alert Letter Response</td>
<td>19</td>
</tr>
</tbody>
</table>

**AGENCY RESPONSE – Technology Services**

| AGENCY RESPONSE – Denver Police Department | 32 |
EXECUTIVE SUMMARY

Police, Fire, and Sheriff Department Electronic Records Are At Risk of Total Loss Should There Be a Data Center Disaster

Critical Police, Fire, and Sheriff computer systems reside in a data center that offers little to no assurance that it can recover from a disaster. Of eight serious backup and recovery concerns, the most notable are the failure to send backup files offsite and the failure to provide enough disk space for the data backup server. In addition, there are several other important issues concerning user administration, antivirus and system patching, data center security, and change management.

Backups Are Not Stored Offsite

Critical Police, Fire, and Sheriff computer systems have their data backed up to disk on a server that resides within the same data center. No additional copies of the data are stored offsite. The close proximity of the backup files being located just a few feet away from their primary system, along with the absence of any automatic fire suppression in the Safety data center, almost assures their mutual destruction in the event of a fire or other disaster. The fact that there is neither a written disaster recovery plan, nor are there any tests scheduled to demonstrate recovery capability for the Police Records Management System (RMS) exacerbates this issue.

It is best practice to store backup files far enough away from their primary systems so that neither location would be subject to the same hazards, such as fire, broken water pipes, or a tornado. It is also best practice to develop recovery plans to allow operations to resume in the event of a disaster.

Dangerously Low Disk Space Threatens the Viability of System Backups

Our testing of routine RMS data backup processing showed an unusually large number of failed backup tasks. Upon closer examination we discovered that the backup tasks were failing because the backup server had run out of disk space.

A data center fire would assure the mutual destruction of both primary and backup records.

The backup server ran out of disk space causing backup jobs to fail on eleven consecutive days.

Although Technology Services Department (Technology Services) personnel have long been aware of Citywide disk space shortages, they were caught off guard by the severity of the shortage in the Safety data center due to a sudden growth in disk space consumption and the lack of a dashboard or automated reporting of performance monitoring metrics. While the person responsible for monitoring the successful completion of backup jobs went on vacation, there was a span of eleven days when no RMS data backups completed successfully. Technology Services
management only became aware of the severity of the issue when it was brought to their attention by our auditors.

The City Auditor alerted the leaders of the City’s Safety Departments on October 4, 2012 that there are serious shortcomings in its backup capabilities that require immediate remediation. Please see Appendix A for a copy of the City Auditor’s alert letter and Appendix B for a copy of the response from Technology Services.

Overall there are eight issues identified for the broad topic of backup and recovery indicating a regrettably low process maturity in a fundamental control area. Technology Services and the Denver Safety Departments need to collaborate to address these critical shortcomings. Of highest importance is the need to relocate the backup server offsite from the Safety data center. Secondly, the issue of disk space capacity must be resolved.

**User Administration Controls Do Not Ensure Timely Termination of Access or Adequate User Activity Monitoring**

Administrating system accounts or user IDs is important to ensuring system access is appropriate, that segregation of duties is maintained, and that access is adjusted when employees transfer within or separate from the City. Criminal Justice Information Services Security Policy also require that access and usage of police systems be reviewed weekly for anomalies.

Our testing identified that missing procedures, errors in programming logic, and insufficient logging have contributed to omissions in maintaining appropriate system access, failures in disabling accounts, and the absence of RMS user activity monitoring. The Police Department and Technology Services must work together to adjust procedures, investigate and resolve discrepancies, and provide adequate monitoring of RMS user activity.

**System Software Patches and Antivirus Updates Are Not Monitored for Successful Installation and Sometimes Not Applied At All**

System software patching and antivirus updates are two fundamental controls that when not performed can leave entire systems vulnerable to exploitation, attack, and damage. We found that missing procedures and insufficient data radio bandwidth have resulted in unresolved patch and update failures, systems being out of date, and in some systems being unprotected. Technology Services and the Police Department should collaborate on improving procedures and identifying technical solutions for patch and update management.

**The Safety Data Center Has No Automated Fire Suppression and Lacks Adequate Physical Access Controls**

The Safety data center was constructed within a converted office space in a building that did not initially have the types of environmental controls and physical protections of modern facilities. Although the Safety data center has been retrofitted with air conditioning, network infrastructure, and electrical power, it has no automated fire
suppression and lacks adequate physical access controls and procedures. Technology Services and the Denver Safety Department should collaborate to address the fire suppression and physical security issues.

**Minor Project Change Management Does Not Provide Adequate Segregation of Duties**

The Denver Police Department works directly with the RMS vendor to implement minor software fixes and customizations that do not require extensive project monitoring or testing. However, procedures do not prohibit the same person from requesting, approving, and testing the changes before implementation. Nor do the procedures require that any of the minor changes be documented. This could result in unauthorized changes and difficulties in determining what changes were made should a system problem arise. The Denver Police Department should modify its procedures to support segregation of duties and require documentation for the changes it requests and implements.

**INTRODUCTION & BACKGROUND**

**What Is a Records Management System?**

A records management system (RMS) is “an agency-wide system that provides for the storage, retrieval, retention, manipulation, archiving, and viewing of information, records, documents, or files pertaining to law enforcement operations. RMS covers the entire life span of records development – from the initial generation to its completion. An effective RMS allows single entry of data, while supporting multiple reporting mechanisms.”

**The Denver Police Department RMS**

The Denver Police Department has been using the Versatern RMS since 2002. The system can be accessed from desktop computers and from laptop computers, known as mobile data terminals (MDTs), which are installed in police cars. Versatern contains general offense records including officer statements, neighborhood surveys.

---


2 Versatern is a Canadian software vendor that specializes in systems supporting police, fire, and emergency medical services.
and lab reports. RMS also interfaces with other City systems, including the Computer Aided Dispatch (CAD) system operated by the City’s 911 Communications Center.

As one of the Denver Police Department’s main records system, RMS is accessed by approximately 1,700 users, including 1,400 sworn police officers, and personnel from other agencies, such as the District Attorney, City Attorney, Denver Sheriff, and Denver County Courts.

**Criminal Justice Information Services Security Policy**

As RMS contains criminal justice information, it must be managed and protected according to the requirements set forth by the Federal Bureau of Investigation (FBI) through its Criminal Justice Information Services (CJIS) Security Policy. The policy provides a minimum set of security requirements associated with the creation, viewing, modification, transmission, dissemination, storage, or destruction of criminal justice information.

**Safety Data Center**

The computer servers that run RMS are located in a City data center managed by the City’s Technology Services Department. Referred to as the “Safety data center” in this report, it also houses other critical public safety systems used by the Police, Fire, and Sheriff Departments, including the Jail Management System, the Office of System Integration, and the High Activity Location Observation (HALO) video recorders.

**What Are IT General Controls?**

Information Technology (IT) general controls are those “behind the scenes” processes and procedures, both manual and automated, that serve as a foundation for the proper operation and security of information systems. General controls are implemented at the policy, physical, and technical levels. An example of a policy control is requiring all persons to be accountable for their access to systems. This is implemented through a physical control that restricts and logs access to the data center by way of a card reader. A technical control supporting accountability is the use of user IDs and passwords to gain access to systems.

General controls are also implemented through processes and procedures, such as one called provisioning, which includes the assignment of user accounts, the granting of access permissions, and the removal of access when personnel transfer or terminate their employment with the City. Other general controls include the physical security of the data center and its backup and recovery procedures.³

**The Importance of Backups**

The operation of the Police Department’s RMS depends on the continuous availability and proper functioning of four key components: facilities, machines, software, and data.

---

Each component must be backed up so that they can be recovered in the event that any of them are damaged or malfunctions. There must be plans to recover the data center facility and its associated network infrastructure at an alternate location if the primary data center becomes unusable due to a fire, for example. The computer servers are amongst the machines that need to be replaced if they become damaged or malfunction. The configurations of the operating system (Linux), database system (Oracle), and RMS application are the software components that must be backed up in order to restore the system in the recovery environment. Lastly, the RMS data must be restored into the database before the system can be returned to use.

As there are various methods to create backups, the overall recovery strategy for a business system should be derived from a risk assessment that takes into account the criticality of the system, how much data it processes, how long the business can tolerate the system being unavailable, and how recent the backup needs to be when the system is restored, amongst other factors. Outcomes from the risk assessment will dictate how often the system should be backed up and how exceptions or backup failures will be handled and reported to the business owners.

Techniques used to backup a system can vary based on risk or available financial resources. A high risk system may require that it be continuously backed up to a duplicate server that can be accessed the instant a problem occurs on the primary system. Systems of lower risk, or those with fewer financial resources, may use a combination of monthly full and once-a-day incremental backups.

A full backup is a copy of the entire database. An incremental backup is a copy of a single day’s work. In the event the database needs to be restored, the most recent full backup would be used as the starting point with the subsequent daily incremental backups applied. This would restore the database up to the point of its most recent backup. The effectiveness of this backup approach requires that each full and incremental backup completes successfully. Without successful backup completion, there will be gaps in the data that could cause the restored database to be incomplete and possibly unreliable.

The risk assessment will also help guide the business to decide how many generations of backups should be kept and how long data should be retained. Backup files are typically retained in generations, sometimes referred to as the “grandfather, father, son” method. The most recent backup is called the “son,” with the previous or next older backup being called the “father,” and the oldest backup being called the “grandfather.” In this three-generation example, the “grandfather” generation is overwritten by the next “son” generation, and so forth, so as to recycle the media upon which the backups are stored. Backups can also be kept based upon a data retention schedule. For example, some systems may require that data be kept for a certain number of years, according to various policies or regulations.
SCOPE

Audit work focused on the controls over account provisioning, logical access, activity monitoring, system and antivirus update and patching, mobile device security, backup and recovery, service level performance, data center security, and change management. These controls were reviewed to varying degrees as applicable at the RMS application, Oracle database, and Linux server levels.

OBJECTIVE

The purpose and overall objective of the audit was to examine and assess the IT general controls related to the Police Department’s Records Management System to ensure that they provide a sound foundation to support the system’s proper operation and security.

METHODOLOGY

We utilized several methodologies to achieve the audit objective. Our evidence gathering techniques included, but were not limited to, the following:

- Consulting the Criminal Justice Information Services (CJIS) Security Policy
- Conducting interviews with personnel in both the Technology Services and Denver Police Departments to obtain an understanding of RMS processes
- Examining job completion results for full and incremental backups for RMS servers and data
- Reviewing root cause analysis documentation for RMS system outages
- Extracting system and password configuration settings for the Oracle database supporting the RMS application
- Evaluating the access permissions granted for privileged Oracle database accounts
- Verifying that default passwords have been changed on privileged Oracle database accounts
- Verifying that the password configurations for the Oracle database are in accordance with the CJIS Security Policy
- Reviewing change management procedures for the RMS application
- Interviewing the RMS vendor for documentation supporting small change requests
• Reviewing Windows Server Update Services (WSUS) reports to determine the current status for the critical and security patches
• Reviewing McAfee ePolicy Orchestrator (ePO) reports to determine the rate of success for anti-virus updates
• Arranging for the scan of attachments and documents stored in the RMS database for any malicious software utilizing the Clam AV (antivirus) tool
• Determining whether police mobile data terminals (MDTs) have had software patches and antivirus updates installed
• Verifying that access to the administrative functions on the police MDTs is appropriately restricted
• Independently testing the physical security of MDTs in a sample of police vehicles
• Evaluating the proxy server configuration and MDT browser settings to determine that Internet access is appropriately restricted
• Consulting best practices for security, backup, and recovery from the National Institute for Standards and Technology (NIST) and the Federal Information System Controls Audit Manual (FISCAM)
• Examining RMS password configurations for compliance with CJIS Security Policy and the City’s Acceptable Use Policy
• Verifying that administrative access to RMS is limited to authorized individuals
• Using Computer Assisted Audit Techniques (CAATs) to compare the population of 3,394 users with access to the RMS application with the population of active employees in PeopleSoft HR to identify terminated users whose system access has not been disabled
• Independently utilizing the Active Directory Users and Computers (ADUC) tool and indirectly using both the Hyena Active Directory analysis tool and the Quest log analysis tool to examine user account and activity information
• Reviewing whether rules were defined in the Cisco Monitoring, Analysis, and Response System (MARS) to monitor logical access activities for RMS application
• Monitoring the execution of scripts to extract system and password configuration settings for the Linux application server
• Directly observing physical and environmental controls in place at the Safety data center
• Verifying that access to the Safety data center was limited to authorized individuals
• Determining whether written contingency plans exist for the RMS application to include business risk assessments, backup and recovery strategies, and whether tests are scheduled to demonstrate any recovery capability
FINDING 1

Police, Fire, and Sheriff Department Electronic Records Are At Risk of Total Loss Should There Be a Data Center Disaster

The combination of backup files not being stored offsite, along with failures in creating backups, seriously jeopardizes the capability to recover critical Safety Department systems and records should there be a data center disaster. The fact that there is neither a written disaster recovery plan, nor are there any tests scheduled to demonstrate recovery capability for the Police Records Management System (RMS) exacerbates this issue. Eight issues contribute to the risk of total loss of electronic records in the event of a Safety data center disaster.

**Backups Are Not Stored Offsite**

In the Safety data center, we found that the RMS backup files are located just a few feet away from their primary system. The Safety data center also lacks an automatic fire suppression system, almost assuring the mutual destruction of the primary system and its backup files in the event of a fire or other disaster. It is best practice to store backup files far enough away from their primary systems so that neither location would be subject to the same hazards, such as fire, broken water pipes, or a tornado. Although offsite backup is common in other areas of the City, the Police, Fire, and Sheriff Departments have not had their backups stored outside of the Safety data center due to interpretations of access restrictions mandated by the Criminal Justice Information Services (CJIS) Security Policy. We recognize the mandated access controls but do not interpret them to prohibit offsite storage of backups. For example, the backups could be stored at a police district station and still maintain a protected enclave in compliance with CJIS requirements.

**Dangerously Low Disk Space Threatens the Viability of System Backups**

RMS data is backed up using a method of full and incremental backups. Our testing of routine RMS data backup processing showed an unusually large number of failed backup tasks or jobs. Upon closer examination we discovered that the backup tasks were failing because the backup server had run out of disk space. There were periods of up to eleven consecutive days where both full and incremental data backups failed without anyone

![RMS Database Backup Job Completion Results](image)

*Figure 2 - Calendar showing incremental and full backups. Job failures are shown in red.*
being aware, as the person responsible for monitoring the tasks was on vacation. Since Technology Services management was not aware that the backup processes were not completing, no one in the Police Department was informed that recovery capability was impaired during this period. Had there been a need to recover from a backup during this period, several days’ worth of data may have been lost, adversely affecting current Police Department operations. Further, incomplete data may cause the database to become unreliable or cause certain records to become corrupted and unusable.

At the time of our testing, the backup server space was over 98 percent full with approximately one half of one terabyte of available space remaining to provide backups for all Safety Departments. To put this in context, some people have more free space on their home computers than does the backup system for the entire Police, Fire, and Sheriff Departments combined. When pricing a new home computer, one can increase the disk space from one to two terabytes for only $75. This comparison to home computer data space and pricing is simply intended as a point of reference. Unfortunately, adding capacity to the enterprise backup systems currently in use is not as simple as adding a disk drive, nor can it be done for $75. In fact, the complexity and high cost of enterprise backup systems is a contributing reason why the backup problem exists.

Technology Services has long been aware of Citywide disk space shortages, but they were caught off guard by the severity of the shortage in the Safety data center due to a sudden growth in disk space consumption and the lack of a dashboard or automated reporting of performance monitoring metrics.

The City Auditor alerted the leaders of the City’s Safety Departments on October 4, 2012 that there are serious shortcomings in its backup capabilities that require immediate remediation. Please see Appendix A for a copy of the City Auditor’s alert letter and Appendix B for a copy of the response from Technology Services.

**Summary of Backup and Recovery Concerns**

Overall there are eight serious issues identified under the broad topic of backup and recovery, which indicates that the process maturity for this fundamental internal control area is regrettably low. Summaries of the eight issues follow.

**Offsite** – Backups are not stored offsite, away from the primary Safety data center. In order to recover from a data center disaster, backups must be accessible from a place not affected by the same disaster in order to re-establish operations at another location.

**Disk Space** – There is insufficient disk space available for backups. Technology Services personnel have identified that a significant portion of the existing backup capacity is
taken up by data that must be saved for legal purposes. They have been able to free up some disk space by moving those files to tape. However, in spite of their best efforts, the demand for backup disk space is close to exceeding the space available.

**Key Personnel Dependency** – Backups were not monitored for successful completion due to the unavailability of key staff while on vacation. There is insufficient staffing to assure that co-workers can cover for each other while trying to keep up with their regular workloads.

**Disaster Recovery Plan** – There is no written disaster recovery plan for the RMS system. A written plan is necessary to ensure that all parties are informed and understand their responsibilities in the event of a disaster.

**Disaster Recovery Test** – No tests of recovery capabilities are planned. Even in the absence of a written disaster recovery plan, some tests can be conducted to provide proof of concept with regard to recovery strategies.

**Backup Methodology** – The backup methodology and exception procedures used for RMS are not documented. The frequency of full and incremental backups is not defined. The number of backup generations and the data retention periods are also not documented. Without a procedural standard, management cannot demonstrate that its backup controls are working as prescribed.

**Frequency of Backup** – During the course of our audit, we observed that the frequency of full backups for RMS was reduced from twice per month to once per month. This was done to reduce the demand for backup disk space, which is understandable given the disk shortage circumstances. However, the frequency of backup should be dictated by the business application risk assessment and should not be changed without including the business owner in that decision. Decreasing the number of full backups increases the dependency on incremental backups, which could lead to longer recovery times if they are needed.

**Service Level Agreement** – The service level agreement between Technology Services and the Safety Department indicates that backups will be stored offsite, which does not occur. Also there are no key performance metrics to alert either Technology Services or the Police Department of process failures. Some business processing, like system backups, is run through automation. However, these systems do not interface with a dashboard or another automated reporting system to alert management when important processes fail. Currently, job processing is verified manually. Further, there is no requirement that obligates Technology Services to notify the Police Department of process failures or report on system performance.
RECOMMENDATIONS

Technology Services and the Denver Safety Departments of Police, Fire, and Sheriff must collaborate to mitigate the risk associated with the identified critical backup and recovery shortcomings. Following are eight recommendations that align with the issues listed in Finding 1.

1.1 **Offsite** – Technology Services must relocate the backup server offsite, away from the Safety data center. The new location should be far enough away so that the new location is not subject to the same hazards, such as fire, broken water pipes, or a tornado. The new location should also meet CJIS access control requirements.

1.2 **Disk Space** – Technology Services and the Denver Safety Departments should collaborate to secure the necessary financial resources to acquire adequate disk capacity for backups.

1.3 **Key Personnel Dependency** – Technology Services should ensure that critical job functions and essential duties related to monitoring system backups can still be performed by other staff when key employees are out of the office, such as on vacation. Documenting and operationalizing job duties and procedures will aid those who temporarily take over backup-related job functions.

1.4 **Disaster Recovery Plan** – Technology Services and the Denver Police Department should collaborate to develop an RMS disaster recovery plan.

1.5 **Disaster Recovery Test** – Technology Services and the Denver Police Department should schedule tests of the RMS disaster recovery plan in whole or in part to demonstrate recovery capability.

1.6 **Backup Methodology** – The backup methodology and exception procedures used for RMS should be documented. This would include the frequency of both full and incremental backups, the number of backup generations, and how long backup generations are retained.

1.7 **Frequency of Backup** – Technology Services and the Denver Police Department should collaborate to conduct an RMS risk assessment to determine the appropriate type and frequency of backup that is necessary.

1.8 **Service Level Agreement** – Technology Services and the Denver Safety Department should jointly review their Service Level Agreement to ensure that it is both realistic and understood. Key performance metrics should be identified and automated reporting should be developed to alert both Technology Services and Denver Safety Department management of process failures, such as missed data backups.
FINDING 2

User Administration Controls Do Not Ensure Timely Termination of Access or Adequate User Activity Monitoring

The RMS system consists of user workstations, MDTs in police cars, an application server, a database server, and other components. Each component has its own accounts and methods for controlling access. For example, a police officer using a workstation will log in to Microsoft Windows before starting RMS. The workstation method will utilize a network login that invokes a database known as Active Directory to identify and authenticate the user. On the other hand, a technician who needs to maintain a server will log into Linux which does not use Active Directory. Hence there are a variety of account types that are considered when reviewing access controls. Administering each type of system account or user ID is important to ensuring system access is appropriate and that segregation of duties is maintained. It is also important that account access privileges be updated or removed when employees transfer within or separate from the City.

Our tests of RMS application access included a three-way comparison between the internal RMS system accounts, the employment status of the user in the City’s human resources system (PeopleSoft), and the status of the user accounts in Active Directory. Our sampling identified error rates as high 57 percent, indicating that a selected population of over 900 accounts must be manually reviewed to determine appropriate RMS access and whether network accounts (Active Directory) need to be disabled. A factor contributing to the error rate was that the Information Management Unit within the Police Department was not being notified when employees were transferring within or separating from the City.

We also identified errors in automated process used to deactivate the network access (Active Directory accounts) for certain types of separated employees. In addition, our review of server administration identified that some settings for local user accounts, such as password restrictions, on the Linux servers and Oracle database were not in compliance with either City or CJIS security requirements.

Further, we found that RMS user accounts are not monitored in accordance with CJIS requirements. CJIS specifies that certain types of user activity data are to be collected and reviewed weekly by the Police Department for anomalies in user access or usage of police systems.

Without good controls to ensure timely termination of accounts or access monitoring, it may be possible that accounts of former employees could be used by unauthorized individuals without detection.
RECOMMENDATIONS

Several procedures should be modified to address deficiencies in user access controls, as follows.

2.1 The Denver Police Department should manually review the list of 911 users provided by the auditors to determine the appropriateness of access granted, and disable accounts in RMS as necessary.

2.2 Technology Services should review the results from the Denver Police Department review of RMS access to ensure that the network accounts (Active Directory) of separated users is removed.

2.3 The Denver Police Department should modify its procedures to notify the Information Management Unit when employees transfer or separate to allow the timely removal of their RMS access.

2.4 Technology Services should correct the processing logic of the automated process to ensure that separated users have their network accounts disabled.

2.5 The Denver Police Department should collaborate with Technology Services and the RMS vendor to collect the appropriate data and generate the reports necessary to allow review of user activity in accordance with CJIS requirements (section 5.4.1.1). Further, the Denver Police Department should perform weekly RMS user activity reviews as required by CJIS.

2.6 Technology Services should ensure that local accounts on Linux servers and the Oracle database are administered in accordance with either City or CJIS requirements as appropriate.

FINDING 3

System Software Patches and Antivirus Updates Are Not Monitored for Successful Installation and Sometimes Not Applied At All

System software patching and antivirus updates are two fundamental controls that when not performed can leave entire systems vulnerable to exploitation, attack, and damage. Even a single key system element can become the weakest link and possess the potential to compromise several other controls and threaten the integrity of overall system processing. System patching and antivirus updates must be performed for all systems that access the network including workstations, MDTs, and servers.

We found that a majority of workstations on the Safety Network receive both system patches and antivirus updates. However, no follow-up is performed in the few instances where patches and updates are unsuccessful. We found that none of the Linux servers
supporting RMS run antivirus software and that there is no established vulnerability patching process in place.

We also found that there is no proactive process to provide software patching and antivirus updates for the nearly 500 police cars equipped with Mobile Data Terminals (MDTs). The data radio bandwidth available to the police cars is insufficient to allow successful downloads and updates. Manual update procedures would require more personnel. In one police district, however, we observed that the police cars were equipped with cellular modems and were able to receive some updates, since they had sufficient data speeds. This is the only district in the City to have cellular modems in the police cars, and there are only about twenty-five cars in the district.

However, each MDT is potentially a conduit to introduce a computer virus into the RMS system through an uploaded attachment. We conducted a scan of over one terabyte of attachment data and found no computer viruses.

We also discovered that in 2008 a project was initiated to install wireless access points at ten police locations that would allow police cars to receive software patches, antivirus updates, and other updates while parked nearby.

The project was underfunded as it included only the installation of the wireless access points and did not include funds for purchasing and installing software and other internal processing infrastructure to allow it to become activated. Ten Tropos wireless access points were mounted and provided power, but were not connected to the City’s network. This resulted in about $75,000 in hardware to be underutilized since the system never served its intended use and sits idle to this day.

**RECOMMENDATIONS**

Technology Services should strengthen its system patching and antivirus update procedures to protect against software vulnerabilities and computer viruses as follows.

3.1 Technology Services should develop procedures to ensure that software patching and antivirus updates are applied successfully and that failures are investigated and resolved.

3.2 Technology Services should install antivirus software on all RMS servers including Linux servers.

3.3 Technology Services should adopt software patching procedures for all RMS servers.
3.4 Technology Services and the Denver Police Department should collaborate on solutions for applying software patches and antivirus updates for the nearly 500 MDT-equipped police cars in the City.

FINDING 4

The Safety Data Center Has No Automated Fire Suppression and Lacks Adequate Physical Access Controls

The Safety data center was constructed within a converted office space in a building that did not initially have the types of environmental controls and physical protections of modern facilities. Although the Safety data center has been retrofitted with air conditioning, network infrastructure, and electrical power, it has no automated fire suppression and lacks adequate physical access controls and procedures.

Fire Suppression – Although there are hand held fire extinguishers in the Safety data center, it has no automated fire suppression system. Industry best practices promote the use of automated fire suppression systems in data centers to prevent potential problems that may hinder normal operations. An electrical fire in the Safety data center could spread rapidly and cause extensive damage and destruction of equipment.

Physical Access Controls – Since the Safety data center processes criminal justice information, CJIS requires accountability for those who accesses the facility. This can be accomplished through the use of badge readers and visitor sign-in logs. The facility has two doors: one is equipped with a badge reader while the other is equipped with a pair of small barrel bolt locks, one on both the inside and outside of the door. We found that the outside barrel bolt was not engaged in the locked position. Even when engaged, barrel bolt locks do not provide a record of access. Also, there is no visitor sign-in log to record the presence of persons who do not have regular authorized access to the Safety data center.

RECOMMENDATIONS

Security of the Safety data center should be improved to provide automated fire suppression and enhanced access control as follows.

4.1 Technology Services and the Denver Safety Department should collaborate regarding how an automated fire suppression system can be installed for the Safety data center.
4.2 Technology Services and the Denver Safety Department should collaborate to install a card reader to replace the barrel bolts on one of the Safety data center doors to support accountability for access.

4.3 Technology Services should institute a visitor sign-in log recording access to the Safety data center in compliance with CJIS requirements.

**FINDING 5**

**Minor Project Change Management Does Not Provide Adequate Segregation of Duties**

The Denver Police Department works directly with the RMS vendor to implement minor software fixes and customizations that do not require extensive project monitoring or testing. The absence of a segregation of duties allows the same person in the Denver Police Department to request, approve, and test the changes provided by the RMS vendor. The lack of software change documentation has resulted in neither the Police Department nor the RMS vendor keeping records of the changes requested or implemented.

To ensure that changes are appropriate, there should be a minimal segregation of duties between the requestor and the approver. Further, the Denver Police Department should retain records of changes requested and implemented not only to demonstrate that the changes were authorized, but to provide a history of changes to aid in the investigation of potential system problems.

**RECOMMENDATIONS**

To ensure that minor system changes are properly approved, the Denver Police Department should adopt the following recommendations.

5.1 To provide segregation of duties, the Denver Police Department should require supervisory or other approval of all changes submitted to the RMS vendor.

5.2 The Denver Police Department should retain records of all changes submitted to the RMS vendor along with evidence of approval for both the changes and the test results.
October 4, 2012

Mr. Alex Martinez, Manager of Safety
Mr. Robert C. White, Chief of Police, Denver Police Department
Mr. Gary Wilson, Director of Corrections, Denver Sheriff Department
Mr. Eric Tade, Department Fire Chief, Denver Fire Department
City and County of Denver

Dear Messrs. Martinez, White, Wilson, and Tade,

I am writing to alert you to a serious shortcoming in the backup of your data for all computer systems that you have in the Police Administration Building (PAB) data center. During our current audit of the Police Records Management System (RMS), our auditors noticed an unusual number of failed data backup tasks. Upon closer examination we discovered that the backup tasks were failing because the servers were running out of disk space.

Further research determined that the disk space shortage was not limited to the Police Department, but affected all systems housed in the PAB data center. In addition to RMS, this also included the Jail Management System (JMS), Office of Systems Integration (OSI), PictureLink (mug shots), as well as, all the High Activity Location Observation (HALO) video recordings, amongst others.

Also, all system backups are located within the same data center where the primary system resides and are not stored offsite. As you may know, the PAB does not have a fully automated fire suppression system. In light of the helipad and emergency generator on the roof, it probably has a higher than usual fire risk.

We are currently in the process of preparing an audit report that will highlight these concerns. However, given the seriousness of these issues and the need for immediate remediation of the risk, I felt you should be fully apprised of this issue prior to the report being issued in December.
Appendix A – Auditor’s Alert Letter (continued)

Messrs. Martinez, White, Wilson, and Tade  
October 4, 2012  
Page 2

We understand Technology Services was aware that there was a shortage of disk space, but they were not aware of the failed backup tasks until we notified them of the problem. In the short run Technology Services is trying to free up disk space on the servers to prevent the backup tasks from failing. However, we recommend that Technology Services also relocate the backup servers to another building away from the PAB to allow the restoration of your data should there be a disaster at the PAB.

I recommend you reach out to Mr. Chuck Fredrick of Technology Services to ensure there is a plan to protect your data in the immediate future.

If you have any questions, please call Kip Memmott, Director of Audit Services, at 720-913-5000.

Sincerely,

[Signature]

Dennis J. Gallagher  
Auditor

DJG/sec

cc: Mr. Chuck Fredrick, Chief Information Officer, Technology Services  
Mr. Ethan Wain, Deputy Chief Information Officer, Technology Services  
Mr. William Nagle, Deputy Chief of Administration, Denver Police Department  
Ms. Janice Sinden, Chief of Staff, Denver Mayor’s Office
November 6, 2012

Mr. Dennis Gallagher
Webb Municipal Building
201 West Colfax Avenue
Department 705
Denver, CO 80220

Dear Mr. Gallagher,

I am writing in response to your letter to the Administration dated October 4, 2012, about the shortcomings in the backup of Public Safety data that your team identified during the current audit of the Police Records Management System.

First and foremost, I want to let you know that we take this matter seriously, and that we have for some time. Technology Services projected that we would run into backup issues as early as the fall of 2011, and we issued an RFP for a replacement backup solution that would meet the needs of the entire City and County of Denver, and we are working aggressively to fund this solution. In the meantime, we have or are currently taking several short-term and long-term actions to address the four issues you identified.

Firstly, with respect to inadequate disk space, in the short-term, we are addressing the largest root cause for the backup servers filling up faster than anticipated, which is the unplanned need for litigation hold data. This data is being backed up to tape, where it can be preserved for purposes of litigation hold, but free up space for back-up. Due to the large amount of litigation hold data, this will be an ongoing process, but we have already seen an uptick in space, which has allowed for an increase in the success rates for backups.

Secondly, your team also identified that in the instances where backup tasks failed and alerts were fired by the system, key personnel were not available to correct the issue. There are currently only two system administrators performing backup tasks across the entire City, and this issue was documented while one of those two administrators was out on vacation. The resulting workload overwhelmed the one remaining staff member. Short-term, we have begun cross-training other members of the Technology Services team to perform some tasks during future events. However, this is a band-aid at best. Long-term, we have already identified as part of the Technology Services Strategic Resource Alignment completed earlier in 2012 the need for additional FTE in this area, such that we have more redundancy in these tasks.

Thirdly, your team identified that the frequency of backups have decreased in order to reduce disk space consumption, resulting in greater reliance on incremental backups. Our standard process is to do a full backup monthly and daily incremental backups. Full and incremental backups are taken on a system that has triple checks for reliability. While we do not believe this is an inherent risk OUTSIDE OF THE ISSUES IDENTIFIED ABOVE, we will re-investigate this policy when we have an enterprise backup solution in place where disk space is more plentiful.

Fourthly, it was communicated that backups are made within the same Police Administration Building (PAB) data center and are not stored offsite, presenting a Disaster Recovery risk. Until November of last year with the completion of the Core Network Upgrade, the Safety Network was physically separated from the rest of the City Network, making it impossible to backup to any other facility. We are now in a position to correct this. Short-term, and by the end of 2012, we plan to move the existing Public Safety Backup Server from PAB to an alternate data center, providing for physical separation and reduced risk. Long-term, we plan to advocate for and eventually received the $1.9M in funding required for an enterprise backup solution that would address not only the Public Safety backups, but the larger backup issues across all of the City of Denver.
My last day with the City of Denver is Friday, November 9th. Please feel free to contact Ethan Wain, Deputy CIO or the Michael Wright, Interim CIO with any questions regarding this matter.

Sincerely,

Charles W. Fredrick
Chief Information Officer
City and County of Denver

cc: Mr. Ethan Wain, Deputy CIO, Technology Services
Mr. Michael Wright, Interim CIO, Technology Services
Ms. Janice Sinden, Chief of Staff, Denver Mayor’s Office
Mr. Alex Martinez, Manager of Safety
Mr. Robert C. White, Chief of Police, Denver Police Department
Mr. Gary Wilson, Director of Corrections, Denver Sherriff Department
Mr. Eric Tade, Department Fire Chief, Denver Fire Department
December 06, 2012

Mr. Kip R. Memmott, MA, CGAP, CRMA
Director of Audit Services
Office of the Auditor
City and County of Denver
201 West Colfax Avenue, Dept. 705
Denver, Colorado 80202

Dear Mr. Memmott:

The Office of the Auditor has conducted a performance audit of the Police Records Management System IT General Controls.

This memorandum provides a written response for each reportable condition noted in the Auditor’s Report final draft that was sent to us on November 13, 2012. This response complies with Section 20-276 (b) of the Denver Revised Municipal Code (D.R.M.C.).

AUDIT FINDING 1

Police, Fire, and Sheriff Department Electronic Records Are At Risk of Total Loss Should There Be a Data Center Disaster

RECOMMENDATION 1.1

Technology Services must relocate the backup server onsite, away from the Safety data center. The new location should be far enough away so that the new location is not subject to the same hazards, such as fire, broken water pipes, or a tornado. The new location should also meet CJS access control requirements.

<table>
<thead>
<tr>
<th>Agree or Disagree with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of specific point of contact for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>1/31/13</td>
<td>John Beck x74382</td>
</tr>
</tbody>
</table>

Narrative for Recommendation 1.1

TS plans to move the tape drive system used for archiving to tape to the city’s primary data center as a temporary measure (by 12/31/2012), allowing us to create off-site backup copies. Additionally, we believe we have secured funding to purchase an Enterprise solution that will allow us to back up Safety data to disk stored at an alternative datacenter later in 2013.
**RECOMMENDATION 1.2**
Technology Services and the Denver Safety Departments should collaborate to secure the necessary financial resources to acquire adequate disk capacity for backups.

<table>
<thead>
<tr>
<th>Agree or Disagree with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of specific point of contact for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>03/31/2013</td>
<td>John Beck x74382</td>
</tr>
</tbody>
</table>

**Narrative for Recommendation 1.2**
We believe we have secured funding to purchase an Enterprise solution that will allow us to back up Safety data to disk stored at an alternative datacenter. The need for this system was identified in the TS Strategic Resource Alignment which was presented in May 2012. Additionally, our oldest legal hold has been lifted which could free up around 200TB of storage.

**RECOMMENDATION 1.3**
Technology Services should ensure that critical job functions and essential duties related to monitoring system backups can still be performed by other staff when key employees are out of the office, such as on vacation. Documenting and operationalizing job duties and procedures will aid those who temporarily take over backup-related job functions.

<table>
<thead>
<tr>
<th>Agree or Disagree with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of specific point of contact for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>12/31/2012</td>
<td>John Beck x74382</td>
</tr>
</tbody>
</table>

**Narrative for Recommendation 1.3**
A Backup to the backup administrators has been identified and training is scheduled to be complete by 12/31/12.

**RECOMMENDATION 1.4**
Technology Services and the Denver Police Department should collaborate to develop an RMS disaster recovery plan.

<table>
<thead>
<tr>
<th>Agree or Disagree with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of specific point of contact for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>5/1/2013</td>
<td>John Beck x74382</td>
</tr>
</tbody>
</table>

**Narrative for Recommendation 1.4**
In 2012 TS completed a multi-year project to upgrade the City’s network. One of the reasons for the upgrade was to gain the capability to securely host Safety data at non-Safety buildings. TS is
currently working with Safety on implementing this off-site redundancy. In addition, in our Strategic Resource Alignment presentation, TS included the need (along with the estimated cost) for setting up disaster recovery capabilities in a non-city facility.

**RECOMMENDATION 1.5**
Technology Services and the Denver Police Department should schedule tests of the RMS disaster recovery plan in whole or in part to demonstrate recovery capability.

<table>
<thead>
<tr>
<th>Agree or Disagree with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of specific point of contact for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>3/1/2013</td>
<td>John Beck x74382</td>
</tr>
</tbody>
</table>

**Narrative for Recommendation 1.5**
Once a DR solution has been implemented, it will be tested. A schedule will be set for quarterly testing.

**RECOMMENDATION 1.6**
The backup methodology and exception procedures used for RMS should be documented. This would include the frequency of both full and incremental backups, the number of backup generations, and how long backup generations are retained.

<table>
<thead>
<tr>
<th>Agree or Disagree with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of specific point of contact for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>12/31/2012</td>
<td>John Beck x74382</td>
</tr>
</tbody>
</table>

**Narrative for Recommendation 1.6**
A draft has been created and is in the review process. An initial document will be completed by 12/31/12 and it will be updated when the new enterprise backup system is implemented.

**RECOMMENDATION 1.7**
Technology Services and the Denver Police Department should collaborate to conduct an RMS risk assessment to determine the appropriate type and frequency of backup that is necessary.

<table>
<thead>
<tr>
<th>Agree or Disagree with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of specific point of contact for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>4/1/2013</td>
<td>Todd Deering, 720-913-4831</td>
</tr>
</tbody>
</table>
Narrative for Recommendation 1.7
Enterprise wide risk assessment procedures are being developed and will need to be approved by Executive Leadership. Once policy and procedure have been approved, Information Security Operations will coordinate with Denver Police Department to conduct Risk Assessments as appropriate. A meeting has been set for Dec 5, 2012.

RECOMMENDATION 1.8
Technology Services and the Denver Safety Department should jointly review their Service Level Agreement to ensure that it is both realistic and understood. Key performance metrics should be identified and automated reporting should be developed to alert both Technology Services and Denver Safety Department management of process failures, such as missed data backups.

<table>
<thead>
<tr>
<th>Agree or Disagree with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of specific point of contact for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>4/1/2013</td>
<td>John Beck x74382</td>
</tr>
</tbody>
</table>

Narrative for Recommendation 1.8
TS is going through a full review of the Service Catalog as part of our strategic plan. Once this is done we will begin addressing SLAs. In the meantime, we will create operational level criteria for response and backup methodology.

AUDIT FINDING 2

User Administration Controls Do Not Ensure Timely Termination of Access or Adequate User Activity Monitoring

RECOMMENDATION 2.1
The Denver Police Department should manually review the list of 911 users provided by the auditors to determine the appropriateness of access granted, and disable accounts in RMS as necessary.

<table>
<thead>
<tr>
<th>Agree or Disagree with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of specific point of contact for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>Provided by auditee</td>
<td>Provided by auditee</td>
</tr>
</tbody>
</table>

Narrative for Recommendation 2.1
Agency provides supporting narrative for agreement or disagreement with Recommendation 2.1.

Response to be provided by Denver Police Department.
### RECOMMENDATION 2.2
Technology Services should review the results from the Denver Police Department review of RMS access to ensure that the network accounts (Active Directory) of separated users is removed.

<table>
<thead>
<tr>
<th>Agree or Disagree with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of specific point of contact for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>3/1/2013</td>
<td>Ravi Kumar 720-913-5215</td>
</tr>
</tbody>
</table>

**Narrative for Recommendation 2.2**
RMS is configured manually by pulling the Active Directory account into the requested role on the RMS system. Once this is done, RMS only consults Active Directory for username/password match.

The short term solution is to have CSA and Safety HR Liaisons contact the RMS Systems Administrators to modify access or provision /de-provision manually as needed. This will be completed by 3-1-12.

The long term solution is to engage a CSA Business Analyst to perform role mapping for all RMS access requirements. This will allow us to align these roles with their respective Peoplesoft accounts. At that point RMS can be configured to use this information for authentication and authorization. This will be a time and resource intensive process that we will attempt to fit into the 2013 workplan.

### RECOMMENDATION 2.3
The Denver Police Department should modify its procedures to notify the Information Management Unit when employees transfer or separate to allow the timely removal of their RMS access.

<table>
<thead>
<tr>
<th>Agree or Disagree with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of specific point of contact for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>Provided by auditee</td>
<td>Provided by auditee</td>
</tr>
</tbody>
</table>

**Narrative for Recommendation 2.3**
Agency provides supporting narrative for agreement or disagreement with Recommendation 2.3.

Response to be provided by Denver Police Department.
### RECOMMENDATION 2.4
Technology Services should correct the processing logic of the automated process to ensure that separated users have their network accounts disabled.

<table>
<thead>
<tr>
<th>Agree or Disagree with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of specific point of contact for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>3/1/2013</td>
<td>Ravi Kumar 720-913-5215</td>
</tr>
</tbody>
</table>

**Narrative for Recommendation 2.4**
Same as 2.2 Meeting set for Dec 10, 2012. The solution used for 2.2 will also address this issue.

### RECOMMENDATION 2.5
The Denver Police Department should collaborate with Technology Services and the RMS vendor to collect the appropriate data and generate the reports necessary to allow review of user activity in accordance with CJIS requirements (section 5.4.1.1). Further, the Denver Police Department should perform weekly RMS user activity reviews as required by CJIS.

<table>
<thead>
<tr>
<th>Agree or Disagree with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of specific point of contact for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>5/1/2013</td>
<td>Todd Deering 720-913-4831</td>
</tr>
</tbody>
</table>

**Narrative for Recommendation 2.5**
This requirement will be accomplished with the acquisition of a Security Event and Incident Management (SEIM) solution. Meeting set for Dec 10, 2012 to discuss options with DPD and potential funding sources.

### RECOMMENDATION 2.6
Technology Services should ensure that local accounts on Linux servers and the Oracle database are administered in accordance with either City or CJIS requirements as appropriate.

<table>
<thead>
<tr>
<th>Agree or Disagree with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of specific point of contact for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>3/1/2013</td>
<td>John Beck x74382</td>
</tr>
</tbody>
</table>

- 6 -
Narrative for Recommendation 2.6
Technology Services will centralize LINUX account management and use CF Engine (an open source configuration management tool) to push out account settings. This will ensure that LINUX servers and Oracle databases are administered in a way that meets City and CJIS requirements.

AUDIT FINDING 3
System Software Patches and Antivirus Updates Are Not Monitored for Successful Installation and Sometimes Not Applied At All

RECOMMENDATION 3.1
Technology Services should develop procedures to ensure that software patching and antivirus updates are applied successfully and that failures are investigated and resolved.

<table>
<thead>
<tr>
<th>Agree or Disagree with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of specific point of contact for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>2/1/2013</td>
<td>Ed Vazquez 720-913-4594</td>
</tr>
</tbody>
</table>

Narrative for Recommendation 3.1
This requirement can be met through the acquisition of a Vulnerability Management Tool that integrates with update deployment services and which automates notification of both patch and configuration non-compliance events. TS is currently evaluating this tool to determine if it can be purchased with Payment Card Industry (PCI) Security funds. If so, it will be purchased by 2/1/2013. If it cannot, TS will include it as a 2014 budget request.

TS estimates 90 days from date of purchase to implement the tool and begin monitoring.

RECOMMENDATION 3.2
Technology Services should install antivirus software on all RMS servers including Linux servers.

<table>
<thead>
<tr>
<th>Agree or Disagree with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of specific point of contact for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>3/1/2013</td>
<td>John Beck x74382</td>
</tr>
</tbody>
</table>

Narrative for Recommendation 3.2
CJIS 5.10.4 and FISMA /NIST SP 800-53Ar1SI-3 require malware (virus) protection for all systems accessing, transmitting or storing CHRI. Current host based solution is licensed sufficiently to provide appropriate protection. Non-Microsoft systems were not included in the initial deployment because of limitations in the Management component. The management
component of the host based solution is being upgraded so that protection can be deployed to all systems.

**RECOMMENDATION 3.3**
Technology Services should adopt software patching procedures for all RMS servers.

<table>
<thead>
<tr>
<th>Agree or Disagree with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of specific point of contact for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>3/1/2013</td>
<td>John Beck x74382</td>
</tr>
</tbody>
</table>

**Narrative for Recommendation 3.3**
CJIS 5.10.4 and FISMA/NIST SP 800-53Ar1SI-2 require that all systems controlled by CJIS requirements or that access, transmit or store CHRI be kept up to date and that both software and configuration “flaws” be remediated. Current Police/Sheriff doctrine restricts update opportunities to one time per calendar month for less than four hours across both computing and networking systems, which is inadequate for the required maintenance and upgrades. Current government “Best Practices” (currently in-place at US DoD, US DoS, US DoJ, FBI, USSS, etc.) are:

1. A weekly “maintenance window” of no less than four hours be designated for all systems. Exception process should be put in place to allow for up to 48 hours window delay in the event of ongoing emergency operations and for critical systems to permit alternative weekly maintenance windows to minimize disruption.
2. A mandatory weekly reboot of all client systems (workstations, notebooks, tablets, etc.) and non-essential servers.
3. A mandatory monthly reboot of all essential systems, with an exception process in place to permit alternative reboot schedules as appropriate for the operating platform.

Technology Service will be working with the Departments and Offices within Public Safety to establish a routine sufficient to meet both administrative and technical compliance requirements.

**RECOMMENDATION 3.4**
Technology Services and the Denver Police Department should collaborate on solutions for applying software patches and antivirus updates for the nearly 500 MDT-equipped police cars in the City.

<table>
<thead>
<tr>
<th>Agree or Disagree with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of specific point of contact for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>6/1/2013</td>
<td>Patrick Klein 720-913-4875</td>
</tr>
</tbody>
</table>

**Narrative for Recommendation 3.4**
This item will take both design and funding to be remedied. The possible solutions may include using WIFI points at all the district stations and police headquarters as well as the service
locations to periodically upload updates. Another option may be to utilize wireless through either a Federal/City program or buy contracting with a common carrier. Any of these solutions will require time to work through the funding cycles. TS will begin developing the options in first quarter 2013 with a proposal for the budget cycle in June.

AUDIT FINDING 4

The Safety Data Center Has No Automated Fire Suppression and Lacks Adequate Physical Access Controls

<table>
<thead>
<tr>
<th>RECOMMENDATION 4.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technology Services and the Denver Safety Department should collaborate regarding how an automated fire suppression system can be installed for the Safety data center.</td>
</tr>
<tr>
<td><strong>Agree or Disagree with Recommendation</strong></td>
</tr>
<tr>
<td>Agree</td>
</tr>
</tbody>
</table>

**Narrative for Recommendation 4.1**
Fire Suppression control is chartered to Facilities and is not within the scope of CCD/TS authority. This is part of Public Works work plan in 2013 and we have requested an ETA.

<table>
<thead>
<tr>
<th>RECOMMENDATION 4.2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technology Services and the Denver Safety Department should collaborate to install a card reader to replace the barrel bolts on one of the Safety data center doors to support accountability for access.</td>
</tr>
<tr>
<td><strong>Agree or Disagree with Recommendation</strong></td>
</tr>
</tbody>
</table>

**Narrative for Recommendation 4.2**
Physical access control is chartered to Facilities. We have contacted Stephen Sholler with Facilities and he is working on a solution. This should be completed by 3/31/2013.
RECOMMENDATION 4.3
Technology Services should institute a visitor sign-in log recording access to the Safety data center in compliance with CJIS requirements.

<table>
<thead>
<tr>
<th>Agree or Disagree with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of specific point of contact for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>12/31/2012</td>
<td>Patrick Klein, TS 720-913-4875</td>
</tr>
</tbody>
</table>

Narrative for Recommendation 4.3
A paper log book will meet the requirements and is within CCD/TS Authority. This log book will be placed in the data center and monitored by TS.

AUDIT FINDING 5
Minor Project Change Management Does Not Provide Adequate Segregation of Duties

RECOMMENDATION 5.1
To provide segregation of duties, the Denver Police Department should require supervisory or other approval of all changes submitted to the RMS vendor.

<table>
<thead>
<tr>
<th>Agree or Disagree with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of specific point of contact for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>Provided by auditee</td>
<td>Provided by auditee</td>
</tr>
</tbody>
</table>

Narrative for Recommendation 5.1
Agency provides supporting narrative for agreement or disagreement with Recommendation 5.1.

Response to be provided by Denver Police Department.

RECOMMENDATION 5.2
The Denver Police Department should retain records of all changes submitted to the RMS vendor along with evidence of approval for both the changes and the test results.

<table>
<thead>
<tr>
<th>Agree or Disagree with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of specific point of contact for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>Provided by auditee</td>
<td>Provided by auditee</td>
</tr>
</tbody>
</table>

Narrative for Recommendation 5.2
Agency provides supporting narrative for agreement or disagreement with Recommendation 5.2.
Response to be provided by Denver Police Department.

Sincerely,

[Signature]

Ethan Wain
Technology Services
Deputy Chief Information Officer

cc: Michael Wright, Chief Information Officer
    Sean Curley, Deputy Chief Technology Officer
    John Beck, Director IT Systems
    Pat Klein, Director Network and Telecom
    Ravi Kumar, Director Enterprise Architecture
    Audrey Donovan, Deputy Director Audit Services
    Stephen Coury, IT Audit Supervisor
December 6, 2012

Mr. Kip R. Memmott, MA, CGAP, CRMA
Director of Audit Services
Office of the Auditor
City and County of Denver
201 West Colfax Avenue, Dept. 705
Denver, Colorado 80202

Dear Mr. Memmott:

The Office of the Auditor has conducted a performance audit of the Police Records Management System IT General Controls.

This memorandum provides a written response for each reportable condition noted in the Auditor’s Report final draft that was sent to us on November 13, 2012. This response complies with Section 20-276 (b) of the Denver Revised Municipal Code (D.R.M.C.).

AUDIT FINDING 2

User Administration Controls Do Not Ensure Timely Termination of Access or Adequate User Activity Monitoring

<table>
<thead>
<tr>
<th>RECOMMENDATION 2.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Denver Police Department should manually review the list of 911 users provided by the auditors to determine the appropriateness of access granted, and disable accounts in RMS as necessary.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Agree or Disagree with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of specific point of contact for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>December 14, 2012</td>
<td>Lieutenant John Pettinger</td>
</tr>
</tbody>
</table>

Narrative for Recommendation 2.1

The list of questionable accounts was reviewed. Several were authorized and worked for areas of responsibility that had authorized access to the RMS. Some of the areas of responsibility included the Denver Police Reserves, Denver Safety Cadets, District Attorney’s office, City Attorney’s office,

The review did identify several accounts that were enabled and should have been disabled. The results of the investigation are below:

427 authorized accounts, no change made to the account
484 Separated from the department and the account has been disabled

**RECOMMENDATION 2.3**
The Denver Police Department should modify its procedures to notify the Information Management Unit when employees transfer or separate to allow the timely removal of their RMS access.

<table>
<thead>
<tr>
<th>Agree or Disagree with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of specific point of contact for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>November 5, 2012</td>
<td>Lieutenant John Pettinger</td>
</tr>
</tbody>
</table>

**Narrative for Recommendation 2.3**
The Denver Police Department recognizes the need for better communication between the Human Resource Bureau and the Information Management Unit. A new procedure has been adopted to provide the Information Management Unit timely information within one business day of an employee separation. The notification is handled by the Information Management Unit on the same business day modifying the personnel’s account.

**RECOMMENDATION 2.5**
The Denver Police Department should collaborate with Technology Services and the RMS vendor to collect the appropriate data and generate the reports necessary to allow review of user activity in accordance with CJIS requirements (section 5.4.1.1). Further, the Denver Police Department should perform weekly RMS user activity reviews as required by CJIS.

<table>
<thead>
<tr>
<th>Agree or Disagree with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of specific point of contact for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>Requirement document by 12/31/12 Report completion by 3/30/13</td>
<td>Lieutenant John Pettinger</td>
</tr>
</tbody>
</table>
Narrative for Recommendation 2.5
The Denver Police Department recognizes the need to be compliant with CJIS requirements. A coordinated effort between the Denver Police and Technology Services is required to become compliant. The specifications/requirements can be completed by the end of December and Technology Services can determine the level of effort and deliverable date. An estimate was given for a completion date.

**RECOMMENDATION 5.1**
To provide segregation of duties, the Denver Police Department should require supervisory or other approval of all changes submitted to the RMS vendor.

<table>
<thead>
<tr>
<th>Agree or Disagree with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of specific point of contact for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>November 21, 2012</td>
<td>Lieutenant John Pettinger</td>
</tr>
</tbody>
</table>

Narrative for Recommendation 5.1
The Denver Police Department recognizes the need for segregation of duties. A procedure has been put in place for the Information Management Unit personnel to formalize a 1) request for change 2) documented testing within a test environment 3) request to apply the change to the production environment 4) testing in prod to confirm the change works as expected.

The change management request will be from the Information Management Unit to the Commander of the Administrative Management Division. Approval will be given by the Commander to proceed.

**RECOMMENDATION 5.2**
The Denver Police Department should retain records of all changes submitted to the RMS vendor along with evidence of approval for both the changes and the test results.

<table>
<thead>
<tr>
<th>Agree or Disagree with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of specific point of contact for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>November 21, 2012</td>
<td>Lieutenant John Pettinger</td>
</tr>
</tbody>
</table>

Narrative for Recommendation 5.2
The Denver Police Department recognizes the need for tracking changes and approvals related to the RMS. A procedure has been put in place for proper documentation, approval and testing of the requested changes.

The documentation will be kept electronically and stored on a shared drive for inspection by appropriate staff.
The Denver Police Department appreciates the time that was invested in the audit and bringing these items to our attention. If you have any questions, please contact myself or Lieutenant John Pettinger at 720-913-6410.

Respectfully,

[Signature]

William Nagle
Deputy Chief of Administration
Denver Police Department