City of Santa Fe

AGENDA

REGULAR MEETING OF THE AUDIT COMMITTEE DECEMBER 15, 2021 AT 2:00 PM ATTEND VIRTUALLY

SPECIAL PROCEDURES FOR AUDIT COMMITTEE MEETING

Attendance: In response to the State's declaration of a Public Health Emergency, the Mayor's Proclamation of Emergency, and the ban on public gatherings in excess of those permitted in the current Public Health Order, and the need to incorporate technology and practices to re-institute in-person meetings consistent with the limitations established by the Order, the Audit Committee meeting will be conducted virtually.

Viewing: Members of the public may attend the meeting live on Zoom.
Please click the link below to join the webinar: https://santafenm-gov.zoom.us/j/87030247900?pwd=amhyZ1FpMk9qUEd5a2c5TVdYbFNYUT09
Passcode: 826625
Or Telephone: 253 215 8782 or 346 248 7799
Webinar ID: 870 3024 7900
Passcode: 837906
Agenda: The agenda for the meeting will be posted at https://santafe.primegov.com/public/portal.

1. **CALL TO ORDER**
2. **ROLL CALL**
3. **APPROVAL OF AGENDA**
4. **APPROVAL OF MINUTES**
   a. Audit Committee – October 6, 2021
5. **PRESENTATION**

- Internal Audit Presentation – Information Technology
- Internal Audit Presentation – Police Evidence Room

- 2022 Risk Assessment

6. **NEW BUSINESS**

7. **MATTERS FROM STAFF**

8. **MATTERS FROM THE COMMITTEE**

9. **MATTERS FROM THE CHAIR**

10. **NEXT MEETING:**

11. **ADJOURN**

Persons with disabilities in need of accommodations, contact the City Clerk's office at 955-6521, five (5) working days prior to meeting date.

City of Santa Fe

MINUTES

REGULAR MEETING OF THE AUDIT COMMITTEE OCTOBER 06, 2021 AT 2:00 PM
VIRTUAL MEETING

1. CALL TO ORDER

Audit Committee Meeting called to order 2:06 pm.

2. ROLL CALL

Members Present:
Member Adolfo Montoya
Member Al Castillo
Chair Stephanie Woodruff

Members Excused:
Member Mary Ellen Erpelding-Chacon
Vice Chair Cristina Mulcahy

Others Attending:
Carolynn Roibal, Attendee
Mary McCoy, Finance Director
Fran Dunaway, Attendee
Bradley Fluetsch, Attendee
Alexis Lotero, Attendee

3. APPROVAL OF AGENDA

MOTION: Member Castillo moved, seconded by Member Montoya, to approve the as presented.

VOTE: The motion was approved on the following Roll Call vote:

For: Member Montoya, Member Castillo, Chair Woodruff

Against: None

Abstain: None

4. APPROVAL OF MINUTES

a. Regular Audit Committee – June, 23, 2021

MOTION: Member Montoya moved, seconded by Member Castillo, to approve the June 23rd Minutes as amended to show Al Castillo as present for that meeting.

VOTE: The motion was approved on the following Roll Call vote:

For: Member Montoya, Member Castillo, Chair Woodruff

Against: None

Abstain: None

5. **EXECUTIVE SESSION**

6. **NEW BUSINESS**

a. FY20 Audit Presentation- (Raul Anaya, Principal, CliftonLarsonAllen LLC; Mary McCoy, Finance Director, mtmccoy@santafenm.gov, 505-955-6171, Alexis Lotero, Assistant Finance Director, aclotero@santafenm.gov; 505-955-6137)

Mary McCoy, Finance Director, Alexis Lotero, Assistant Finance Director, Clayton Pelletier, Controller, Brad Fluetsch, Finance Planning and Investment Officer presented an overview of the City of Santa Fe's Financial Performance and update on actions to improve the City's plan to fill vacancies, provide training, tools and technology to staff.

Raul Anaya, Principle Auditor with Clifton Larson Allen (CLA) presented the Audit for June 30, 2020, He gave a summary of the Audit and stated the City of Santa Fe 2020 Audit was given the highest rating that could be given which is an unmodified opinion.

Raul Anaya with CLA also went into depth on the Audit findings at the request of other members of the Audit Committee. Mary McCoy, Finance Director also spoke to the action plan to correct the findings and hiring challenges.

7. **PUBLIC COMMENT**

8. **MATTERS FROM STAFF**

Mary McCoy suggested additional Audit presentations and updates forthcoming in future meetings- and moving forward on action plans related to tlhe findings.

9. **MATTERS FROM THE COMMITTEE**

10. **MATTERS FROM THE CHAIR**

11. **NEXT MEETING: January 05 2022**

    a. TBD

Next meeting to be held January 5, 2022 at 2pm

12. **ADJOURN**

Meeting adjouned 3:02 pm.

Liaison

Chair

City of Santa Fe

Information Technology Internal Audit

April 2021

REDW LLC
CPAs | Advisors

City of Santa Fe
Information Technology Internal Audit

Table of Contents

City of Santa Fe
Information Technology
Internal Audit

Report

INTRODUCTION

We performed the internal audit consulting services described below to assist the City of Santa Fe Information Technology and Telecom (ITT) department in evaluating the policies, procedures, processes and internal controls over various ITT areas including network, physical and workstation security, mobile device usage, user access and ITT Governance to ensure adherence with best practices and sound internal controls.

Our services were performed in accordance with the terms of our Professional Services Agreement and engagement letter for internal audit services and the applicable Standards for Consulting Services prescribed by the American Institute of Certified Public Accountants. Although we have included management's responses in our report, we do not take responsibility for the sufficiency of these responses or the effective implementation of any corrective action.

PURPOSE AND OBJECTIVES

Our internal audit focused on evaluating and testing the City of Santa Fe's ITT controls and security processes, particularly with workstation security, employee education, and incident response and employee access controls.

OBSERVATIONS, RECOMMENDATIONS AND MANAGEMENT RESPONSE

As a result of our testing, REDW identified the following observations:

1) Employee Access

Network access as well as access to individual software within each department is granted by the City's ITT department and a form is completed and signed by the Department Director prior to access being granted. For all terminations, Human Resources is responsible for sending a termination memo to ITT at which point a work order is created to document the removal of network access. Our testing determined:

- Forms and/or work order documentation was not on file for the four transferred employees we tested therefore, we were not able to determine if access had been terminated from their previous positions.

Arizona
5353 N 16th St, Suite 200
Phoenix, AZ 85016
P 602.730.3600

New Mexico
7425 Jefferson St NE
Albuquerque, NM 87109
P 505.998.3200

Oklahoma
708 N Santa Fe Ave, Suite 110-E
Edmond, OK 73003
P 405.543.1410

- 12 of 18 terminated employee accounts were not disabled on the termination date. Variances ranged from 10 to 156 days.
- For 6 of 18 terminated employee accounts, we were unable to conclude the account disable date due to a lack of documentation and inefficiencies in reporting on the helpdesk system.
- 8 of 18 employees did not have a HR termination memo to generate the termination work order. 2 of these 8 had their accounts disabled within 10 to 26 days while the remaining 6 accounts did not have adequate documentation in place to determine the disabled date.

Furthermore, five of the termination memos ITT was able to provide were received from Human Resources approximately one week or longer after the employees had terminated, which is a significant gap in time between actual employment termination and notification of accounts needing to be disabled.

Lastly, we determined there are no procedures in place to ensure departments monitor access to department software to ensure user access is appropriate for job title and function. This is especially critical on software that is web-based and therefore accessible from any device.

Potential Risk: *High* — The absence of a consistent process to ensure transfers and terminated employee access is appropriate increases the risk to high that inappropriate access may be granted for extended periods of time resulting in potential access to sensitive data.

Recommendations:

1. The Computer Access Controls policy was last updated in 2017. Update and enforce the Computer Access Control policy to ensure compliance with end user activation and de-activation for both the City network and systems access. In the policy, expand on both the employee transfer and the employee termination process to include all steps to be taken to successfully complete these processes, and communicate these processes throughout the City.
2. Implement a formal monitoring program for both network and systems accounts to ensure accounts with no activity have been reviewed and/or disabled within 30 days and document the account review process.
3. The formal monitoring program should also include controls over monitoring for department software to ensure individual departments are performing access reviews on a periodic basis (at least annually). In the event they are not performing the reviews, procedures should be in place for the ITT department to work with the department directors to get access removed.
4. Ensure Human Resources notifies the ITT department of voluntary employee terminations before the termination date to confirm network and systems access is disabled the day of termination. Having this information ahead of the termination date will allow the ITT department more time to be proactive with the employee termination process. ITT should be immediately notified of involuntary employee terminations to ensure network and system access is disabled in conjunction with the employee's exit.

Management Response: The Computer Access Control Policy-Authentication and Authorization was reviewed and updated on March 27, 2020. The REDW recommendations will be added to our policy repository for consideration during the next revision of the policy by the end of FY 2022.

2) Employee Security Awareness Training

A formal security awareness training program is in place for all newly hired employees as well as additional procedures that are performed throughout the year such as mock phishing attempts and communications regarding how to handle suspicious e-mails that have infiltrated the network. While the City has an Information Security Awareness and Training Policy that requires security awareness training for all new hires, and annual training for all employees, relevant consultants and contractors, the City has not implemented a formal and mandatory security awareness training program to continuously educate all employees on the risks associated with fraudulent emails, social engineering techniques, website browsing, mobile device security, or other cyber security risks.

During our testing of employee knowledge over security awareness, we identified the following:

- 2 of 15 employees disclosed having clicked links or downloading attachments from questionable email messages and did not know the proper procedure to report questionable email messages;
- 8 of 15 employees did not remember the last time they had security awareness training, or any training received since new hire orientation;
- 13 of 15 employees had remote access but only one out of the thirteen said remote access security training was provided;
- 6 of 15 employees did not know the risks related with USB devices; and
- One employee did not know to contact the ITT department to report a possible security incident but would contact the department supervisor.

Furthermore, multiple employees communicated they do not regularly read the emails sent by the ITT department that contain security training tips and tricks.

Potential Risk: *High* **—** The absence of a formal security awareness training program and consistent education practices to City employees regarding IT threats escalates the risk to high that employee actions could result in a network breach and potentially compromise sensitive data.

Recommendations:

1. Formulate and document a training plan to incorporate onboarding, proactive training and reactive (follow up) training for all employees, temporary workers, and contractors on a continuous basis (i.e., monthly, quarterly, etc.).
2. Consider using an online security awareness training platform that offers:
    - Short user inter-active training modules with follow up questions
    - The ability to send mock phishing emails to employees
    - Provides a secure method for employees to report suspicious messages to the ITT department for review and feedback (usually in the form of an or email plugin)
3. Establish sanctions for non-compliance when employees do not complete training.

4. Ensure management is able to measure employee training performance and set risk indicator scores for the City and employees (i.e., the City and employees will not exceed a risk percentage above 20%).
5. Update the Information Security Awareness and Training Policy with the training plan, sanctions, and risk score once the formal program has been implemented.

Management Response: The City has implemented a training platform called Localgovu that has training modules on Cyber-Security Threats to Public Entities and Protection from Ransomware and Phishing Attacks. IT is currently working with Human Resources to implement those modules in City Wide training. The Localgovu training has testing as part of the training. In addition, as part of our new Cybersecurity/Ransomware Insurance with Cowbell for the year we have committed to using Cowbell's partner Wizer cybersecurity training. We plan on using the current policy and the projects mentioned above to document the cybersecurity training plan by the end of FY 2022.

3) Windows Operating Systems and Updates

The ITT department supports over 1,300 employee workstations that are either connected to the City's network or used by remote City employees. While the majority of the population has been transferred to a new operating system, our testing over workstation security determined three of 15 workstations tested were running on an unsupported operating system and one of 15 workstations had not had Windows updates applied since December 2020. In addition, our testing determined that while updates are configured to automatically install on workstations, this process is not monitored to ensure successful installations.

Potential Risk : *High* — The presence of workstations which run unsupported operating systems increases the risk to high as these systems will not receive critical monthly security updates leaving the systems vulnerable to be compromised. In addition, the absence of a system to monitor the installation of critical security patches further increases the risk as ITT may not be aware of installation failures.

Recommendations: The City should identify and update all unsupported workstations to the most current operating system to ensure they are receiving critical security updates. In addition, a system should be implemented to monitor and alert the ITT department of any workstations that are not current or have failed critical security updates.

Management Response: The REDW recommendations appear reasonable and we will implement by the end of FY 2022. We are monitoring using LabTech and in progress to remediate the issue.

4) Workstation Security

Employee workstation security is a critical component to ensure the protection and security of the City network and confidential data. The ITT department has policies in place to address critical workstation security components such as prohibiting removable media like USB drives and requiring authorized users to obtain encrypted USB drives from ITT. Our testing over workstation security determined:

- All 15 workstations tested could access free proxy server websites which, if installed, will allow an employee anonymous web browsing bypassing City security and monitoring controls;

- Personal e-mail websites such as Gmail, Hotmail, Yahoo, etc. were not blocked on the City of Santa Fe network, which could introduce malware into the network from infected email or provide the opportunity for employees to communicate City information from an unauthorized email account;
- 13 of 15 workstations could access social media websites, which in nature are insecure and without proper social media security awareness training for employees can expose the City and employees to additional security and privacy risks;
- 3 of 15 workstations were using unencrypted non-City of Santa Fe ITT issued USB drives and in one instance, a cell phone plugged into the USB port was not scanned by the monitoring application; and
- One out of 15 workstations had continuously failed to update to the current anti-virus update leaving the machine vulnerable to new malware exploits.

Potential Risk: *High* — The absence of monitoring controls in place over workstation security increases the risk to high that employees could inadvertently download or click on malicious links while on City of Santa Fe equipment. This is further escalated to high due to the absence of security awareness training (See Observation #2).

Recommendations:

1. Block access to free proxy server websites and personal email websites at the firewall level to reduce the risk of employees compromising the City of Santa Fe network.
2. Develop a social media acceptable use policy and determine whether or not all employees are authorized to access social media from the City of Santa Fe network and which sites are acceptable. Include training on the security risks of social media for City employees. Block social media sites from unauthorized employees at the firewall level.
3. Implement automated preventive controls over the use of USB drives. These automated controls can be configured to block the use of unauthorized USB drives on City systems or automatically encrypt the drive if it is not already encrypted.
4. Ensure removable media policies are communicated to all employees as part of their security awareness training.
5. Consider only allowing authorized personnel to use City issued encrypted USB drives for business purposes to ensure City data saved on these drives cannot be accessed if the drive is lost or stolen.
6. Ensure workstation endpoint protection is actively monitored to mitigate possible security incidents that could take place due to the failure of the endpoint protection software not updating.

Management Response: We have implemented controls to block free proxy web servers. We have a policy in place that addresses social media in our technology resource acceptable use policy and plan on implementing a more comprehensive policy. The suggestions from REDW are reasonable and we will work on implementing those controls that are technologically feasible by the end of FY 2022.

5) Mobile Devices

Employees are authorized to synchronize City email to City issued mobile devices (smartphones, tablets, etc.). While, the ITT department has a Mobile Device Acceptable Use Policy outlining access control, device security and hardware support for mobile devices, there is currently no requirement for employees to acknowledge they will comply with the mobile device policies. Our testing determined:

- 2 of 10 employees synchronized City of Santa Fe email to a personal smartphone and one of these employees also acknowledged to downloading attachments to the personal device despite the policy stating only City issued mobile devices can be utilized;
- 8 of 10 employees had not read the mobile device policy and therefore did not understand the City's policies surrounding mobile device usage;
- 1 of 10 employees did not have a PIN or passcode on the City device therefore leaving their phone and City e-mail easily accessible; and
- 2 of 10 employees did not know the proper steps to take if the device was lost or stolen.

In addition, none of the 10 employees we tested were enrolled in the mobile device management solution which assists ITT with the secure management of the devices in addition to the ability to remotely wipe the device in the event of a theft or misplacement.

Potential Risk: *High* — While policies and procedures have been developed over mobile phone usage, they are not actively utilized to educate employees on City policy regarding City issued devices thus leaving the City susceptible to potential compromise by poor mobile device management. This risk is escalated to high as the mobile device management solution is not in place to assist ITT with secure management of the devices in the event of theft or misplacement.

Recommendations:

1. Enroll all City of Santa Fe smartphones into the mobile device management solution to ensure these devices can be securely managed and remotely wiped should the device be lost or stolen. If possible, configure the mobile device management solution to only allow authorized smartphones to connect to the City's email system.
2. Finalize the Mobile-Portable Computing Device Form and ensure employees authorized to use City of Santa Fe smartphones read the Mobile Device Acceptable Use Policy and sign the Mobile-Portable Computing Device Form before being issued their City mobile devices. In addition, the ITT department, in collaboration with City Legal, should review policies surrounding personal devices to determine potential risks associated with allowing employees to utilize their personal device for City e-mail and determine if policies should be updated to reflect only City issued devices will be allowed.
3. Train mobile device users on the security risks associated with mobile devices particularly with email, saving sensitive data on the device, accessing social media sites, downloading, and installing mobile applications, and other cybersecurity risks to help mitigate mobile device security risks.

Management Response: We believe the recommendations from REDW are reasonable and will continue to work on user training, providing copies of mobile device policy and rules forms, and will provide updated information to the end users on a regular basis by the end of FY 2022.

6) Security Incident Response

Data security best practices require organizations to have a formal, written, Security Incident Response Plan that is tested at least annually to ensure the ITT department can respond appropriately to security incidents, retain necessary evidence, and communicate appropriately to necessary parties regarding mitigation of incident risks. While the City of Santa Fe has a documented Security Incident Response Plan it has not been tested to ensure appropriate incident response for possible attack scenarios.

Potential Risk: *High* — Without testing, the City may be ineffective in responding and recovering from a data breach or cybersecurity attack which could be costly to the City.

Recommendations: Management should require the Security Incident Response Plan to be tested at least annually and that testing is documented. Testing can be completed with table top exercises to perform various tasks required to respond to a variety of identified incidents such as unauthorized access, malware, theft or a compromised account. Furthermore, City leadership should take proactive measures and determine should a major incident occur, such as a ransomware attack, what the City is willing to do to get their information back and what are acceptable downtimes for their systems. Planning through this in advance will help the ITT Department respond without having to make these major decisions reactively in the moment.

Management Response: Security Incident Response plan testing is on the ITT plan for the year. The REDW suggested recommendations looks like a good list to incorporate as part of the testing.

7) IT Disaster Recovery

The City of Santa Fe has a documented Disaster Recovery Plan and Business Impact Analysis which assist with identifying mission critical business activities and their associated recovery timelines in the event of a disaster. Our testing determined the Disaster Recovery Plan and Business Impact Analysis have not been updated since 2016 nor has the Disaster Recovery Plan been tested to ensure recovery times and processes are appropriate. In addition, we performed an assessment of the Disaster Recovery Plan and identified the following key elements were missing:

- The plan does not identify who can declare an event a disaster to start the disaster recovery plan process thus increasing the risk that defined leadership during the event of a disaster recovery event may not be present causing potential delays in recovery;
- There is not a communication plan in the event of a disaster to ensure relevant parties are aware of actions steps to take in the event a disaster has been declared;
- The disaster recovery strategy has not been documented to guide IT and other personnel to ensure the recovery process is successful; and
- Training has not been conducted for employees involved in the disaster recovery planning process, which is necessary to ensure everyone on the disaster recovery team is familiar with their recovery roles.

Potential Risk: *High* — The absence of updated plan documents including the Business Impact Analysis, and testing of the Disaster Recovery Plan increases the risk that in the event of a disaster the City could potentially be offline and City operations could be negatively impacted.

Recommendations:

1. Ensure both the Disaster Recovery Plan and Business Impact Analysis are updated to include any recently identified critical business processes or applications along with the required recovery time and recovery point objectives with the key elements identified above.
2. The disaster recovery strategy should be tested at least annually and testing should be documented. Testing can be completed either with table top exercises or functional recovery of different areas and applications. Testing will help ensure the City will be able to effectively recover from a declared disaster.

Management Response: Updating the Disaster Recovery plan is a high priority for the department. The plan is to hold a workshop this year to update the DR plan, hosted by the same research group that helped with the last DR plan. A DR testing plan will also be developed and testing will take place by the end of FY 2022.

8) IT Governance

IT Governance directs the IT function and strategy and assists with ensuring leadership and executive management are tuned into the IT operations and verifying they are aligned with overall strategic and business objectives City-wide. Best practice recommends governance meetings occur at least quarterly to allow for collaborative discussion on IT strategy and objectives. Our testing determined the IT Governance Committee meetings have not been held since 2017 due to turnover at the City. In addition, we determined there is no City-wide strategic plan to benchmark the IT Governance strategy and function.

Potential Risk: *Moderate* — The absence of a strong IT Governance function increases the risk that IT strategy may not be aligned with City-wide goals and objectives thus potentially resulting in failure of IT projects, over/under spending on IT resources, and the absence of accountability over the IT function.

Recommendations: ITT, in collaboration with City management, should review the IT Governance Charter to ensure it is reflective of best practices and procedures. An IT Governance Committee should be identified and quarterly meetings should be established. Minutes should be kept at each to ensure documentation of topics discussed. Lastly, the City should develop a strategic plan to ensure individual departments can align goals and objectives to overall City goals and objectives.

Management Response: IT Governance process and implementation is a high priority for the IT department and plan on implementing that as soon as possible. We are conducting IT governance using Change Control Board, budget review and informal meetings and will work on re-implementing a more formalized process by the end of FY 2022.

9) Standard user agreements

When a new employee is hired at the City, they are required to read and understand the acceptable uses of the City of Santa Fe technology resources and sign the Technology Resources Standard User Agreement which is then kept on file in the Human Resources department. Our testing determined 4 of 20 employees did not have their form on file. Communication with HR indicated there is no process in place to ensure this form is obtained upon hire.

Potential Risk: *Moderate* **—** The absence of a signed acknowledgement demonstrating employee agreement with technology resource policies increases the risk that employees may not be aware of City policies and therefore may inadvertently violate security protocols.

Recommendations: The ITT department, in collaboration with HR, should implement a process to ensure the Technology Resources Standard User Agreement form is signed by all new hires prior to providing access to network resources.

Management Response: We will assist Human Resources as requested to help support any controls needed including document retention by the end of FY 2022.

10) Remote Access

The City has implemented a secure remote access connection for authorized employees to utilize while working remotely. Employees who wish to obtain remote access must complete an authorization form and obtain approvals prior to access being granted. The ITT department, in accordance with the Remote Access Policy, must keep records of these forms on file. Our testing determined 19 of 20 employees did not have record of a remote access authorization on file either in the help desk ticket system or email archives.

Potential Risk: *Low* **—** The absence of authorization forms to document approval of remote access increases the risk that employees may not have department director approval prior to obtaining remote access.

Recommendations:

1. Ensure all employees configured for remote access have an approved authorization form on file indicating remote access is allowed. This includes any employees that were configured for remote access before the 2017 Remote Access Policy went into effect.
2. Disable all remote access accounts for employees who are not authorized for remote access or no longer need to use remote access for their job function to mitigate unauthorized access to the network.

Management Response: We are working on a strategy to mitigate the concerns documented by REDW. With ongoing Covid Pandemic telecommuting this is an issue that we will work with executive leadership to maintain both security and access as needed by the end of FY 2022.

11) IT Policies and Procedures

Policies and procedures are critical for the ITT department to ensure both ITT and City employees have clear understanding of what City requirements are surrounding several areas and processes over the IT environment. The National Institute of Standards and Technology (NIST) has several IT related best practices including what policies an IT department should have in place. During our testing over policies and procedures, we determined the ITT department has developed and approved 27 of the 31 recommended policies by NIST. The following policies had not been approved as of testing but are currently in draft form:

- Data Classification Policy
- Physical Security Policy
- Social Media Acceptable Use Policy
- Vendor Management (IT) Policy

In addition, of the 27 policies in place, 13 have not been reviewed since 2017 and one, the Technical Resource Acceptable Use Policy has not been reviewed since 2003, however, the ITT department is currently in process of reviewing outdated policies and is targeting one policy per week to get them up to date with current procedures and best practices.

Lastly, we identified several policies where policy components may be missing in accordance with NIST best practices.

Potential Risk: *Low* — While some policies are in draft form and others are outdated, ITT has already implemented procedures to update all policies thus reducing the risk to low.

Recommendations:

1. Ensure the Technical Resource Acceptable Use policy is updated to include new processes, new technologies, and IT best practices that have been implemented since policy creation to better manage employee expectations with acceptable use of the City's technology resources.
2. Establish controls to ensure all City employees have reviewed and signed the Technology Resources Standard User Agreement at the time of hire to mitigate technology risks.
3. Review and update policies annually, or as technology best practices are updated and new controls are implemented for the City to keep technology policies and procedures current.
4. Finalize the draft Data Classification, Physical Security, Social Media Acceptable Use, and Vendor Management policies to continue meeting best practice security standards.
5. Review each policy as well as the NIST best practices and consider implementing the components identified to ensure adherence with best practice.

Management Response: We will continue to update and add additional policies as recommended by REDW. The Technology Resources Standard User Agreement has been updated and is being reviewed by executive leadership. We will continue to build communication with other stakeholders to help expand policies where relevant by the end of FY 2022.

SCOPE AND PROCEDURES PERFORMED

In order to gain an understanding of the processes and operations, we interviewed the following personnel:

- Manuel Gonzales, Interim ITT Department Director
- Bradley Purdy, Chief Information Security Officer
- Larry Worstell, IT Infrastructure Services Manager
- Edward Duran, ITT End User Services Manager
- William Smith, IT Architect
- Felix Herrera, System Administrator
- Ramon Cameron, ITT End User Support Technician

In order to gain an understanding of the IT infrastructure, controls, policies and procedures, we read relevant portions of:

- City of Santa Fe Information Technology policies and procedures
- ITT Organizational Chart FY20
- The City of Santa Fe ITT Disaster Recovery Plan Report 2016, and the Infrastructure 2021 City of Santa Fe Disaster Response Summary
- Incident Response and Investigation Checklist SOP and Incident Response – Malware & Viruses SOP
- ITT Strategic Roadmap 2015 – 2018, and the ITT FY21 Strategy and the ITT Strategy Portfolios Programs Projects
- ITT Budget Procedures for FY21 (June 2020)
- IT Governance Charter
- IT Governance Committee
- City of Santa Fe IT Security Awareness Training materials (October 27, 2020)

We performed the following test work:

IT Governance – We obtained an understanding of the IT Governance function and obtained the IT Governance Charter. We evaluated whether the documentation was in alignment with IT best practices based on NIST standards with a specific focus on:

- A strong reporting structure and defined roles and responsibilities
- Involvement of City executive leadership at regular intervals
- Alignment of the ITT strategic plan to the City's business plan
- Contribution of ITT goals to the business strategic objectives
- The ITT strategic plan covered the operational budget for ITT

In addition, from the documentation we determined whether:

- There was a standing IT agenda item at executive leadership meetings
- All ITT personnel had signed a confidentiality / non-disclosure agreement at the time of hire

Policies and Procedures — We obtained the policies and procedures in place over the IT function and tested to determine if they had been reviewed on an annual basis. In addition, we performed a gap analysis based on the NIST and International Organization for Standardization Frameworks to determine if critical components were present in the policies.

IT User Agreements — We obtained a listing of all employees in place as of March 2021. From a total population of 1,251 employees, we selected 20 and tested to determine if the Technology Resource Standard User Agreement was signed by each employee at the time of hire and was retained in the employee file.

User Access Controls- New Hires — We obtained a listing of all new hires that occurred between June 1, 2020 and March 19, 2021. From a total population of 44 new hires, we selected 5 and tested to determine:

- The access form was completed and approved; and
- Access was granted timely after completion of the form.

User Access Controls- Transfers — We obtained a listing of all transfers that occurred between June 1, 2020 and March 19, 2021. From a total population of 38 transfers, we selected 4 and tested to determine:

- The approval form authorizing the change was submitted and approved; and
- The change was made properly in the system and old access was removed.

User Access Controls- Terminations — We obtained a listing of all terminations that occurred between June 1, 2020 and March 19, 2021. From a total population of 179 terminations, we selected 18 and tested to determine:

- A request to disable access was completed; and
- Access was disabled on or prior to the termination date.

User Access Reviews — We obtained an understanding of controls in place over user access to determine if annual reviews are performed to ensure user access is aligned with job title and function.

Workstation Security — We obtained a listing of all employees as of March 2021. From a total population of 1,251 employees, we selected 15 employees with a specific focus on employees who utilize IT resources daily. We then tested to determine:

- Employees did not have administrator rights on their computer;
- Security patch/update and virus pattern updates were current;
- The operating system was current;
- Controls over password protected screen savers were in place;
- The user was not able to access proxy and social media websites; and
- Security controls were in place when a USB device was plugged into the computer.

Employee Security Awareness — We gained an understanding of processes in place to ensure employees are aware of potential network security threats. Utilizing the sample selected in the Workstation Security testing, we interviewed each employee to determine:

- When they last received security awareness training;
- If they used VPN for remote access and had been trained on remote access use and security;
- If they synchronized their smartphone to City of Santa Fe email;
- If they were aware of:
    - How to recognize a security incident and where to report it
    - Social engineering techniques

- Password security and creating a strong password
- Dangers related to USB devices, and
- Risks related to email and phishing attacks

We also determined if controls were in place to monitor suspicious e-mails and filter them accordingly.

Mobile Device Security — To evaluate security controls over sensitive data on mobile devices and removable media, we utilized the sample of 15 employees from above. From the 15 employees, 10 were identified as syncing City of Santa Fe email to their mobile devices and tested to determine:

- If the employee had a PIN, biometric, or password enabled on the device;
- If the employee sends, downloads, or receives sensitive information by email;
- What the employee would do if the device was lost, stolen, or compromised; and
- If the employee had been provided and read the Mobile Device policy.

In addition, we gained an understanding of what controls are in place to monitor mobile devices issued to employees.

IT Disaster Recovery Plan — We obtained the Disaster Recovery Plan, the Business Impact Analysis, and the backup and restoration policies and procedures. We assessed each for the following:

- The plan was documented and reviewed annually;
- A Business Impact Analysis had been completed and there were calculated recovery point objectives (RTO) and recovery point objectives (RPO) for all critical apps;
- A Disaster Recovery Plan risk assessment had been completed;
- Roles and responsibilities for those involved were identified;
- The plan identified who declares an event a disaster and starts the disaster recovery process;
- There was a current call tree for employees and vendors/outside entities;
- There was a communication plan for a disaster;
- The disaster recovery strategy had been documented;
- There were detailed procedures for recovery of critical systems;
- There was an alternate site in place;
- There were back up processes in place;
- The plan had been tested annually and testing had been documented with an after-action report; and
- Annual training was conducted for all involved in the disaster recovery process.

Additionally, we selected 15 critical data backup logs from September 1, 2020 through March 31, 2021, and tested to determine the backup schedule was followed and the backup process was successful.

Security Incident Response Plan — We obtained the Security Incident Response Plan (SIRP) and policies and tested the plan to determine:

- The plan was up-to-date and adequate for responding to a cyber incident
- The plan identified a SIRP owner with defined duties
- A SIRP team had been identified along with the SIRP team's responsibilities and duties
- The plan included testing and training requirements
- The plan contained computer security incident classifications (i.e., unauthorized access, theft, compromised account, malware, etc.)
- There was a security incident notification process
- The plan contained incident severity classifications (high, low, etc.)
- There was an investigation process and included a physical evidence handling, copying, preservation, and retention processes
- There was containment, eradication and recovery processes
- The plan included a communication and reporting process

Additionally, we tested to determine if the plan had been tested and the SIRP team had been trained on their role.

Physical Security — We obtained an understanding of the data centers' physical security controls, and tested the physical security policy and procedures to determine physical controls were in place for IT work areas, data centers, server rooms, telecommunication closets as well as general access to City of Santa Fe buildings. Furthermore, we determined if the policy addressed environmental controls and fire suppression for data centers and server rooms.

Remote Access Security — We obtained the remote access policies and procedures and gained an understanding of processes in place. We then obtained a listing of all remote access users as of March 2021. From a total population of 415 remote access employees, we selected 20 and tested to determine if remote access was monitored and proper remote access documentation had been completed and approved.

* * * * *

This report is intended solely for the information and use of City of Santa Fe's management, Audit Committee and City Council members. If additional procedures had been performed, other matters might have come to our attention that would have been reported to you.

We received excellent cooperation and assistance from City of Santa Fe personnel during the course of our testing. We very much appreciate the courtesy and cooperation extended to our personnel. We would be pleased to meet with you to discuss our findings and answer any questions.

REDW LLC

Albuquerque, New Mexico
August 24, 2021

City of Santa Fe

Santa Fe Police Department Evidence Unit

Internal Audit

June 2021

REDW LLC
CPAs | Advisors

City of Santa Fe
Santa Fe Police Department Evidence Unit
Internal Audit

Table of Contents

City of Santa Fe
Santa Fe Police Department Evidence Unit
Internal Audit

Report

City of Santa Fe
Audit Committee and Management

INTRODUCTION

We performed the internal audit consulting services described below to assist the City of Santa Fe Police Department Evidence Unit in evaluating compliance with policies, procedures, state statutes, and other relevant guidance as well as to assess the adequacy of internal controls over evidence management and evidence collection & preservation. We also evaluated the Evidence Unit's progress towards obtaining accreditation status by the International Association of Property and Evidence (IAPE) and adherence to action plan items as noted in a February 2020 Corrective Action Plan press release.

Our services were performed in accordance with the terms of our Professional Services Agreement for internal audit services and the applicable Standards for Consulting Services prescribed by the American Institute of Certified Public Accountants. Although we have included management's responses in our report, we do not take responsibility for the sufficiency of these responses or the effective implementation of any corrective action.

PURPOSE AND OBJECTIVES

Our internal audit focused on obtaining an understanding of the Santa Fe Police Department's progress towards obtaining accreditation status by the International Association of Property and Evidence (IAPE) and progress with various steps in the Corrective Action Plan, including implementation of modern evidence management software, disposition and destruction of evidence practices, staffing and training needs, improvement of security and access controls to evidence holding areas, and improvement of storage solutions.

Additionally, we evaluated compliance with policies, procedures, state statutes, and other relevant guidance to assess the adequacy of internal controls over evidence management and evidence collection & preservation.

Arizona
5353 N 16th St, Suite 200
Phoenix, AZ 85016
P 602.730.3600

New Mexico
7425 Jefferson St NE
Albuquerque, NM 87109
P 505.998.3200

Oklahoma
708 N Santa Fe Ave, Suite 110-E
Edmond, OK 73003
P 405.543.1410

OBSERVATIONS, RECOMMENDATIONS AND MANAGEMENT RESPONSE

During the course of the audit, we evaluated progress with the Corrective Action Plan and determined for all five priority areas included in the plan, significant progress had been made by the department towards completing the actions necessary to improve operations, staffing and security at the Evidence Room. As a result of our testing, REDW identified the following observations:

1) Evidence Management Policies and Procedures

Policies and procedures are critical to ensuring employees are aware of department procedures surrounding evidence collection, processing, and destruction. In addition, since the SFPD is actively pursuing the International Association for Property and Evidence (IAPE) accreditation, policies and procedures are critical to ensuring processes are documented in accordance with accreditation standards. The Santa Fe Police Department currently has two policies surrounding evidence and property management including Policy 51.1 – Collection and Preservation of Evidence and Policy 52.1 – Evidence Management. Our testing determined both policies are outdated and do not sufficiently outline policies, procedures, best practices, and operations to manage the Evidence Unit in order to meet IAPE Standards.

Potential Risk – High: The absence of updated policies and procedures over evidence collection, processing, and destruction escalates the risk that SFPD employees may not be process evidence in compliance with state and local statutes or accreditation standards.

***Recommendations*:** SFPD should perform a review of the policies and procedures over evidence collection, processing and destruction and update them to ensure they are in compliance with federal, state, and local state statute. In addition, the IAPE provides guidance regarding proper policy and procedure development to ensure alignment with standards for accreditation. We recommend SFPD reference those guidelines and ensure the appropriate standards are infused into the policies to assist with achieving and maintaining accreditation.

Management Response: In response to the recommendations of the pre-accreditation review completed by SCS Northwest Consulting Services, two things needed to be completed prior to implementation of the policies and procedures of the department. The first thing that needed to be done was that the staffing needed to be increased and a permanent supervisor needed to be hired for day-to-day supervision in that section. The second issue that needed to be addressed was all staff, to include the lieutenant who administers the section, would need to attend the latest class for evidence technicians put on by the accrediting organization, International Association of Property and Evidence (IAPE). The lieutenant and the newly hired supervisor would also need to attend the evidence supervisor class. This would ensure that the entire section and its supervisors were aware of the current industry standards and had access to up-to-date information and resources available through IAPE. Staff will also be required to attend the class every two years to stay up to date on the latest training and network with evidence personnel from around the country. Since the above action items have been completed, Evidence staff are currently working with the Administrative Lieutenant on updating the policies and procedures for the section now that we know what the industry standards are and have access to help from IAPE. In addition, we have obtained model policies from other state agencies who are accredited to assist us with getting these implemented. We anticipate the policies and procedures to be completed by end of fiscal year 2022.

2) Packaging and Property Manuals

Proper packaging of evidence is critical to ensuring it is stored properly and also does not pose a risk to those tasked with tagging, moving, and storing it. Our testing determined there are no policies and procedures in place over proper packaging of evidence to ensure officers submitting evidence can reference the processes. As a result, several instances were mentioned where evidence such as narcotics and hypodermic needles, had not been packaged properly and had put the Evidence Technicians at risk of exposure. In addition, while we were onsite performing fieldwork, an envelope containing bullets was not properly secured so when it was removed from the box, the bullets fell out of the packaging.

Potential Risk – High: The absence of policies and procedures over proper packaging of evidence increases the risk that exposure to hazardous drugs and drug paraphernalia may occur, posing a health/safety risk. Additionally, improper, or inconsistent packaging can lead to evidence being lost, destroyed, or accidentally tainted.

Recommendations: A Packaging Manual should be drafted, approved for use, distributed in hard copy and electronic format, and trained on regularly. The manual should address the most common types of property and evidence encountered in the field and should contain photos and directions that are clear, concise, and easy to follow. These guidelines should be disseminated in a manner that all persons who book property/evidence have access to the guidelines. Infractions for non-compliance should be consistent and enforceable agency-wide, regardless of position, seniority, or tenure.

Management Response*:* Evidence staff have completed videos of how to properly package items that are commonly taken in as evidence. Those videos will be available on a YouTube channel that will be available to officers. A sheet with QR code shortcuts to the videos will be placed in all common areas, evidence processing locations and offices. A packaging manual is also in development to accompany the videos and will be available on the police department computer network. While the videos are already available, we anticipate the packaging manual to be completed by the end of fiscal year 2022. The right of refusal has already been instituted for improperly packaged evidence. This means that the evidence technicians may refuse to accept improperly packaged evidence. When this happens the evidence technician sends an email to the officer that they need to correct the issue on their next duty day and tells them exactly what the problem was. The officer contacts evidence staff who then bring the item back to the officer for correction. If the officer needs assistance the evidence staff or crime scene staff will assist them if needed. The email is also copied to the evidence chain of command as well as the officer's chain of command as a record of the issue. Once the correction is made an email from the evidence technician is sent to the respective chains of command stating that the issue has been resolved. It is up to the officer's chain of command to address any disciplinary measures for infractions. The expectations of evidence handling by officers as well as the disciplinary measures for infractions will be documented in the policies and procedures, which are expected to be implemented by the end of fiscal year 2022.

We have also standardized all evidence packaging across the entire department. All packaging is now ordered through the evidence supervisor to ensure this. We have also identified and ordered new packaging that addresses the safety issues identified in the audit.

3) Chain of Custody

Chain of Custody refers to the chronological documentation of the seizure, custody, control, transfer, and disposition of evidence. Policy 52.1 – Evidence Management states that it is the policy of SFPD to ensure the proper chain of custody of each evidence item from the time the property was stored until its final disposition. Our testing determined:

- For 1 of 15 cases tested, 6 of the 9 items related to the case were indicated as being checked out to the DPS Crime Lab when in actuality the items were physically located in the Evidence Unit.
- For 1 of 20 cases, case evidence was documented as checked out to the court when in actuality it was located in the Evidence Unit but had never been signed back in when it was returned.
- For 1 of 20 cases, case evidence was documented as being checked out to an officer. The Transfer to Officer document and lab receipt were attached to the case record, but the record was not updated when the evidence was returned by the officer.

In addition, we determined there is no centralized e-mail address for officers to submit requests for evidence movement and supporting documentation. Instead, officers submit directly to individual Evidence Technicians. As a result, when we inquired about specific cases, it was difficult for the Evidence Technicians to pull up relevant information and extra time had to be spent trying to track the information down.

Potential Risk – High: Failure to completely and accurately track the movement of evidence can potentially expose cases to a defense challenge deeming evidence worthless, which may result in lessened charges and/or increased settlement payouts.

Recommendations: A diversion or chain of custody policy needs to be written and implemented to ensure that all releases and dispositions of property or evidence are legal and accurately documented. The policy should provide directives for any officer signing out or signing in evidence for interim releases and returns of evidence for court, crime lab analysis, or other investigative uses. Infractions for non-compliance should be consistent and enforceable agency-wide, regardless of position, seniority, or tenure. Additionally, a centralized email address for the Evidence Unit should be set up for officers to submit relevant documentation, requests, and/or inquiries to ensure that information is not lost or misplaced in individual Evidence Unit Technician's inboxes. This will also ensure that documentation, requests, and inquiries are received and processed timely regardless of the mix of staff present in the Evidence Unit on a given day. Lastly, periodic training should be implemented over the Chain of Custody process to ensure officers are aware of the importance of maintaining an accurate and complete record.

Management Response*:* As the new staff start to deal with the older cases in the AS400 system they are verifying locations and updating them in the new system. If they are not located, we have been checking the last verifiable person who had custody and completing an investigation on the item's whereabouts. If we still can't locate the item, we are referring the case to Professional Standards for further investigation. We have also created new intake locations downstairs where items are scanned to until they are place in their final locations in the room.

It was also noted that one case was documented as being checked out to an officer with the required paperwork attached to the case record, but the paperwork showing the return was not updated. Officers are now required to scan and attach the return receipts to the record or provide a copy to the evidence technicians to scan and attach to the record. If it is not provided it will be refused by the evidence technician and the officer and chain of command will be notified.

It was also noted that there is no centralized email address for officers to submit requests for evidence movement. The EvidenceOnQ system that we now use has a request function for all evidence movements. This is monitored daily by the evidence technicians. There is no need to use email. Requests are also added automatically to the system's internal audit trail for all evidence and are part of each item's record to include the date and time of the request and when it was fulfilled. The system also requires that anyone taking evidence provide an electronic signature on the MobileOnQ device or a sign out sheet can also be printed and then scanned into the system as part of the record. The system also allows any email correspondence to be attached to the file record for each case. However, all requests must be submitted through the EvidenceOnQ system. Email requests are not accepted.

It was also recommended that evidence handling and chain of custody training was provided to officers on a periodic basis. We wholeheartedly concur and hope to add this to biennium training. We are in the process of building out our training calendar for 2022 and evidence handling/chain of custody will be included. We have already had the crime scene staff conduct rollcall training on this.

4) Annual Comprehensive Review

Policy 52.1 – Evidence Management requires an annual audit of property held by the agency to be conducted by an employee not routinely or directly connected with property control. Our testing determined no annual audits have been performed over the property and evidence functions to ensure all property is accounted for.

Potential Risk – Moderate: The absence of comprehensive annual audit to ensure evidence is inventoried properly increases the risk that evidence may be missing or not in the proper location. This risk is reduced as there are review performed quarterly on a small sample of cases to ensure evidence is inventoried correctly.

Recommendations: SFPD should implement an annual audit in accordance with their policies and procedures. The audit should be documented and signed off on including the date in which it was completed. In addition, since the department is actively pursuing IAPE accreditation, employees should reference the requirements for reviews/audits including the frequency and scope, and infuse those requirements into their policies and procedures.

Management Response*:* It was noted that the Evidence Management policy requires an annual property audit to be completed by an employee not routinely or directly connected to property control. As time allows the staff have been converting the old inventory over to the new storage and evidence system. As this is occurring, the staff have discovered that there have been discrepancies in the old AS400 system and the handwritten evidence sheets located with the cases with there often being more evidence listed on the handwritten evidence sheets as opposed to logged into the system. This will be a very time-consuming process to correct the issues and

get them entered into the new system. Once that is completed the EvidenceOnQ system has an audit function built in that allows for all of our periodic and annual audits that is streamlined and able to use a handheld MobileOnQ scanner that can document them and they can be done very quickly.

One of the issues we have run into with getting this process started is the purge of old evidence that was pointed out in the pre-accreditation report. Our plan was to identify cases that can no longer be prosecuted due to the statutes of limitations and obtain a blanket destruction order from District Court. We did complete a spreadsheet of all the cases that are past the statutes of limitations. Originally, we had met with the District Attorney's Office who had agreed to go through our list of cases to make sure there were no issues on their end for the purge of those on the list. They would then assist us in drafting the requested destruction order and get it approved by a District Court judge. Once the order was signed, we had a company identified that would assist us with the purging of the identified and approved cases on the order. We would then begin the process of converting the remaining inventory over to the new storage and evidence tracking system, which in turn would allow us to complete a timely and accurate annual audit.

The District Attorney's Office has since advised us that they will not look at our purge list until the large amount of disposition orders that had not been processed prior to the new staff being hired has been completed. This is approximately 15 years of disposition orders. The staff have been attempting to start this, but they have discovered that some of the old orders address cases with multiple suspects, yet only one suspect is listed on the disposition. This requires the evidence technician to go to the court website to check the status of charges on all the suspects and verify it with the DA's Office. Another ancillary result of this is that the department now have to assign staff to work on this while our inventory continues to grow exponentially. In order to combat this new issue, we will have to request more staff positions to keep up with what's coming in and also request money to build a new facility to store the expanding inventory. Not including our old inventory that should be able to be purged, we have about 3 items coming in for every item we have going out to destruction. Even with the new storage system we are out of room. With the current staff it will take years for us to process the old orders however, we are actively working with the DA's Office to identify a solution which will hopefully remedy this soon.

5) Evidence Ready for Destruction

There are several considerations that must be made prior to evidence being destroyed including the status of the case, statute of limitations or the level of charges. In most cases a court order is required however, certain types of property for which an owner cannot be identified and the evidence is not tied to a court case is collected and destroyed or disposed of regularly. Our testing determined 2 of 20 samples tested that were marked as ready to destroy could not be located in the Evidence Unit. These pieces of evidence did not have a court case attached to them nor had an owner been identified, and appear to have been destroyed but not documented during the first round of destructions following the implementation of the new evidence management system.

Potential Risk – Moderate: The absence of a process to ensure evidence ready for destruction is periodically reconciled to ensure all items are accounted for increases the risk that evidence tagged for destruction may go missing or items may be destroyed but not properly updated on the evidence logs.

Recommendations: The Evidence Unit should continue to streamline and refine the process for evidence that is ready to be destroyed or disposed of. Evidence tagged as "for destruction" should be audited or inspected regularly to ensure that the items have not been removed from the Evidence Unit, whether accidentally or intentionally. Destructions should continue to be done at set times, or when inventory levels reach a certain amount.

Management Response*:* It was noted that 2 out of 20 items marked for destruction sampled could not be located. Since the visit the staff have created locations for items ready for destruction which the items are now scanned into. A regular schedule of times for destruction has been implemented and two employees then do a scanned audit of each location to verify that all the items are accounted for. Those audits are tracked in the system. Narcotics are verified by our staff and also by State Police staff prior to incineration and a signed copy of each list is kept on file by both agencies.

PROCEDURES PERFORMED AND INFORMATION GATHERED

In order to gain an understanding of the processes and operations, we interviewed the following personnel:

- Benjamin Valdez, Deputy Chief of Police
- Sean Strahon, Lieutenant
- Roberto Romero, Evidence Unit Supervisor
- Amanda Randow, Evidence Technician
- Cassandra Tapia, Evidence Technician

In order to gain an understanding of the processes, we read relevant portions of:

- Santa Fe Police Department Policy 51.1 – Collection and Preservation of Evidence (defective July 23, 2004)
- Santa Fe Police Department Policy 52.2 – Evidence Management (effective May 15, 2017)
- Special Orders
  - Evidence Submission and Management Protocol (dated October 4, 2019)
  - Summary Review on Evidence Unit/Update Evidence Submission and Management Protocol (dated January 10, 2020)
  - Sane Exam Kit Evidence Procedure (dated May 13, 2020)
  - EvidenceOnQ (dated November 4, 2020)
  - New Evidence Unit Schedule (dated November 30, 2020)
  - EvidenceOnQ Red Flag (dated February 9, 2021)
  - Supplemental Reports & Evidence (dated April 26, 2021)
- Progress Reports
  - October 2019
  - November 2019
  - December 2019
  - January 2020

  - February 2020
  - March 2020
  - July 2020
- Comprehensive Evidence Room Project Update (dated March 4, 2021)
- Timeline of Evidence Management Improvements (dated January 20, 2020)
- Evidence Room Project Breakdown (dated February 21, 2020)
- Purchase Requests
  - High Density Mobile Shelving System (date February 19, 2020)
  - Evidence Freezers (dated February 13, 2020)
  - Replacement Temporary Evidence Lockers (dated February 13, 2020)
  - Camera, Security, and Alarm System (dated February 12, 2020)
  - EvidenceOnQ Evidence Management Software (dated February 12, 2020)
  - Evidence Purge Services (dated February 21, 2020)
- New Mexico Records Retention Act
- 2011 New Mexico Statute – Section 29-1-13 – Unclaimed property; inventory
- 2011 New Mexico Statute – Section 29-1-14 – Unclaimed property; authority to sell; notice of sale; deadly weapons, controlled substances and other contraband excepted.
- 2011 New Mexico Statute – Section 30-1-8 – Time limitations for commencing prosecutions
- 2006 New Mexico Statute – Section 6-10-3 – Payment of state money into treasury; suspense funds.
- City of Santa Fe Job Descriptions
  - Evidence/Property Supervisor
  - Evidence/Property Technician
- International Association of Property and Evidence Standards
- Public Safety Committee Minutes – February 18, 2020
- Regular Meeting of the Governing Body Minutes – February 26, 2020
- Various news articles and press releases

Independent consultant's report dated January 3, 2020.

We performed the following testwork:

Corrective Action Plan: We gained an understanding of the Department's progress in relation to their Corrective Action Plan released in February of 2020. The Corrective Action Plan contained five areas we considered throughout our testing:

- Implementation of a modern evidence management software
- Disposing of all inventory that can lawfully be discarded
- Adding additional staff to the Evidence Unit

- Improving security and access control to evidence holding areas
- Improving storage solutions in the evidence holding areas

Utilizing additional reports prepared by an independent consultant as well as the International Association of Property and Evidence (IAPE) Standards, we furthered our understanding of the issues facing the department. We then performed inquiries with SFPD employees to determine progress in each area and identified areas for additional detailed testing which is documented in the procedures below.

Evidence Tagging and Logging: We selected 50 cases from a total population of 2,296 that have gone through the data validation process as of June 2021 listed on the EvidenceOnQ report and 15 cases directly off the shelves. We tested to determine:

- The bin location reflected in EvidenceOnQ (evidence management system) was the same location that the bin was physically located;
- The inventory listing exported from EvidenceOnQ correctly and accurately reflected the items contained in the evidence bin.

Evidence Ready for Destruction: We selected 20 cases from a total population of 178 cases that had evidence flagged as ready for destruction or had previously been destroyed or disposed of. We tested to determine:

If evidence disposition was not case related

- Item was destroyed and inventory listing agreed to disposition worksheet, or,
- Item was still onsite and locations, item description and case number agreed to system listing.

If evidence disposition was case related

- A court order was submitted and signed for destruction/disposition;
- A disposition worksheet had been filled out and was maintained for documentation purposes.

Cash Deposits: We selected 10 deposits from a total population of 103 deposits made from September 30, 2020 through June 21, 2021, and tested to determine:

- Amount on cash transfer log matched amount on deposit receipt;
- Money was transferred to the Cashier's Office on the same day or following day of receipt of cash in accordance with NMSA 6-10-3;
- Deposit receipt was attached to the case in EvidenceOnQ;
- Currency log was signed by two different individuals;
- Amount on cash transfer log agreed to information in EvidenceOnQ; and
- Proper segregation of duties were executed in the counting or cash, the preparation of the deposit, and auditing of deposit.

Documentation of Movement: We selected 20 cases from a total population of approximately 300 cases that were released to an owner, transferred to an outside agency, lab, or court, or released to another individual and tested to determine a Chain of Custody or Diversion Form record was in place and contained:

- The date of transfer and location;
- The receiving person's name and functional responsibility;
- Reason for transfer;
- The name of trying court (if applicable); and
- The name and location of the examining laboratory (if applicable).

Reviews and Audits: We obtained copies of all monthly audits performed since November 2020, and tested to determine that:

- Results of inspections, audits, and inventories were retained;
- Surprise audits were performed at least monthly;
- Corrective actions were documented and retained.

In addition, we tested to determine if annual audits over the evidence population were performed in accordance with policies and procedures.

Access and User Management: We obtained a listing of all employees with access to the evidence holding areas and security systems as of June 2021. We then tested to determine if those listed were current employees and that access was appropriate. In addition, we determined if there was a process in place to revoke or edit access permissions as a result of a termination, transfer, or promotion.

Digital Evidence Management: We gained an understanding of current practices surrounding digital evidence and related IPRA and eDiscovery requests. Additionally, we performed a walkthrough of the new digital evidence management system that the Police Department has been demoing since late 2020 in order to gain an understanding of how the potential software will improve processes and internal controls over digital evidence.

Sexual Assault Exam Kits: We obtained an audit report export which contained a listing of 18 kits submitted to the Evidence Unit in 2020. From this listing, we tested to determine:

- The location in EvidenceOnQ was consistent with the indicated location on the Santa Fe Police SAEK Log utilized for tracking kits on a weekly basis;
- A Chain of Custody Report existed in EvidenceOnQ for the particular kit and the date of check-in to the Evidence Unit agreed to the date on the Santa Fe Police SAEK Log;
- The DPS form was kept on file and the transfer date agreed to the intake date on Chain of Custody report; and
- The kit was physically located in the Evidence Unit's dedicated storage area.

* * * * *

This report is intended solely for the information and use of City of Santa Fe's management, Audit Committee and City Council members. If additional procedures had been performed, other matters might have come to our attention that would have been reported to you.

We received excellent cooperation and assistance from City of Santa Fe personnel during the course of our testing. We very much appreciate the courtesy and cooperation extended to our personnel. We would be pleased to meet with you to discuss our findings and answer any questions.

Albuquerque, New Mexico
December 14, 2021