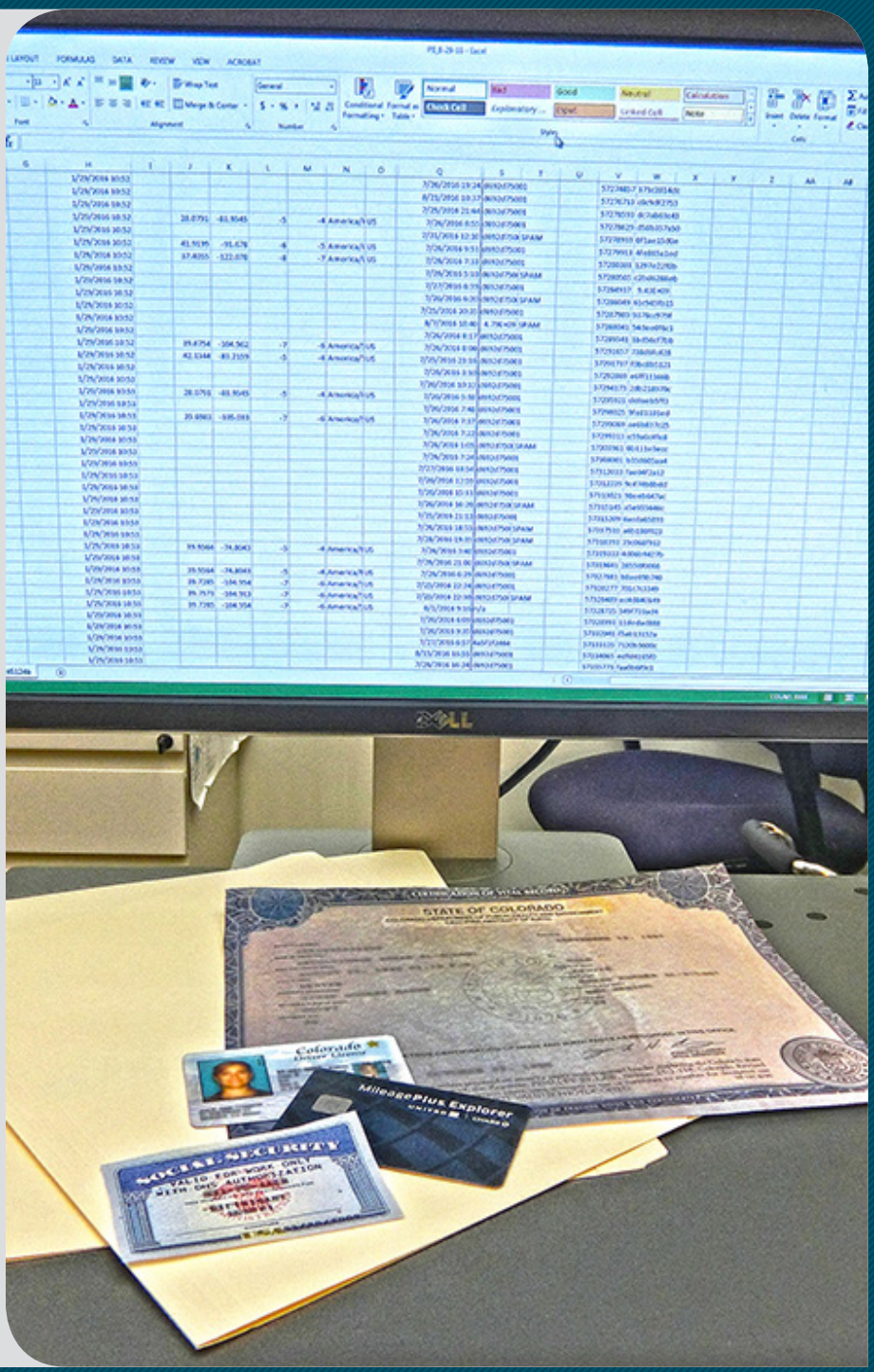
AUDIT REPORT
Citywide
Personally Identifiable Information
December 2016

Office of the Auditor
Audit Services Division
City and County of Denver

Timothy M. O'Brien, CPA
Denver Auditor



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

Timothy M. O'Brien, CPA, Chairman
Rudolfo Payan, Vice Chairman
Jack Blumenthal
Leslie Mitchell
Florine Nath
Charles Scheibe
Ed Scholz

Audit Management

Valerie Walling, CPA, CMC®, Deputy Auditor
Heidi O'Neil, CPA, CGMA, Director of Financial Audits

Audit Staff

Shannon Kuhn, CISA, IT Audit Supervisor
Nick Jimroglou, CISA, Lead IT Auditor
Jared Miller, CFE, Lead Auditor
Karin Doughty, CISA, Senior IT Auditor
Tyler Kahn, Senior IT Auditor

You can obtain copies of this report by contacting us:

Office of the Auditor
201 West Colfax Avenue, #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
Report number: **A2016-010**

City and County of Denver

201 West Colfax Avenue, #705 • Denver, Colorado 80202

720-913-5000 • Fax 720-913-5253 • www.denvergov.org/auditor

Timothy M. O'Brien, CPA
Auditor

December 15, 2016

AUDITOR'S REPORT

We have completed a Citywide audit of personally identifiable information management. The purpose of the audit was to examine the effectiveness of the City's internal controls in place to safeguard personally identifiable information, or PII.

As described in the attached report, our audit revealed that the City does not have a comprehensive Citywide strategy for safeguarding PII that is gathered by several City agencies. We found evidence of unsecured network folders and hardcopy records containing thousands of pieces of PII. We believe that this breakdown in internal controls occurred due to outdated policies and inconsistent practices for safeguarding PII. Through stronger policies, guidance, communication, and training, the City will have the necessary controls in place to safeguard PII, thereby preventing opportunities for identity theft and reducing the City's exposure to reputational damage or costly litigation. Our report lists several related recommendations that, if implemented, will establish a robust framework for PII management based on widely accepted principles and practices.

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.

We extend appreciation to the Mayor's Office and the personnel who assisted and cooperated with us during the audit.

Denver Auditor's Office

Timothy M. O'Brien, CPA
Auditor

REPORT HIGHLIGHTS

Personally Identifiable Information

December 2016

Scope

The audit reviewed the City and County of Denver's practices for collecting, handling, protecting, and disposing of personally identifiable information (PII).

Background

The City and County of Denver collects PII through various agencies that provide services to the public. Types of services provided by the City include, but are not limited to, pet licensing, property tax exemptions for seniors, discounted parks and recreation programs, public assistance, marriage licensing, and the restaurant inspection ride-along program.

Purpose

The objective of the audit was to examine the effectiveness of the controls the City has established to safeguard personally identifiable information.

Highlights

The audit found that the City does not have a strategic framework for protecting personally identifiable information (PII). Specific areas of concern include the following:

- Unsecured network folders containing PII
- Outdated policies and inconsistent practices among agencies
- No comprehensive inventory of intake points for PII or resultant storage locations
- Low completion rate for the City's annual security training, which includes general concepts such as safeguarding and protecting PII
- Lack of public transparency regarding how PII is collected and stored

Without an effective strategy for protecting PII there is an increased risk of unauthorized use or exposure of this data. This can be costly for the individual whose data is compromised, as well as to the City in the areas of potential litigation and reputational harm. We offer several recommendations to mitigate these risks.

For a complete copy of this report, visit www.denvergov.org/auditor

Or contact the Auditor's Office at 720.913.5000

TABLE OF CONTENTS

INTRODUCTION & BACKGROUND **1**

SCOPE **9**

OBJECTIVE **9**

METHODOLOGY **9**

FINDING **11**

The City Should Establish a Strategic Framework to Better Protect Personally Identifiable Information 11

RECOMMENDATIONS **18**

APPENDIX **20**

AGENCY RESPONSE **22**

INTRODUCTION & BACKGROUND

What Is Personally Identifiable Information?

Personally identifiable information (PII) is data that distinguishes an individual, such as full legal name, maiden name, or social security number. One piece of PII alone is not useful for distinguishing an individual unless it is linked to other PII. Linked data makes it possible to trace an individual's identity. For example, a person's date of birth would not distinguish one individual from another unless combined with other PII, such as name, drivers' license number, photo identification, fingerprints, home address, or health and financial information, which provides further specifics about an individual. Since PII is considered to be sensitive in nature, laws and other regulations were established to prevent abuse and fraud.

City Collects Both Publicly Accessible PII and Private PII

Governmental entities collect many types of PII for the provision of services to the public, ranging widely in sensitivity and use. Information collected by the City and County of Denver (City) can be categorized in one of two ways: publicly accessible information and private information. Publicly accessible information is not protected from access by the general public and not considered sensitive in nature. For example, much tax information, such as an individual's property tax history, is publicly accessible, as are home values. Some of this type of information is accessible on the City's website. The Treasury Division's Denver Property Tax Information webpage displays owner's names, addresses, and legal descriptions of homes. There are no laws preventing this information from being made publicly available.

Private information, on the other hand, is protected and thus should not be publicly accessible. In the government context, this would be PII that individuals are asked to provide when filling out forms for government-provided services or assistance. For instance, when applying for a marriage license, an individual must provide one of the following types of identification: a U.S. state-issued driver's license, other type of state-issued ID, U.S. military ID, or U.S. passport and a social security card, if the person is a resident of the U.S. This information is collected by the State of Colorado and is considered private.

The City's Use of PII

There are a variety of reasons for the City to collect PII. In some cases, it is necessary to ensure eligibility and to correctly identify individuals who apply for services or benefits. For example, the City administers programs that benefit disadvantaged residents, such as child welfare, food assistance, and temporary assistance for the elderly or for people living with a disability. In other instances, the City collects information on illness, disease, and death occurring in the population through the Office of the Medical Examiner.

Collection of PII by City Agencies

Several City agencies collect PII; however, some agencies collect more than others based on their strategic goals. This audit focused on the agencies that collect the most PII. The audit team identified the following agencies as collecting more than one kind of PII, such as residency status, U.S. citizenship or qualified alien status, social security number, and legal name: Denver

Human Services, Office of Economic Development, Treasury, Parks and Recreation, and Environmental Health.

Each City agency has its own webpage hosted on the Denvergov.org website, which many agencies use for collecting information. Some agencies use embedded forms that contain fields, such as *name* and *address*, which the user fills out directly on the webpage. Once the form is completed, the data is submitted directly to a City web application or hosted application. Other agencies use forms that, once completed, must be printed and mailed or hand delivered to the agency. Whether collected via the internet or in person, agencies must store, retain, and eventually dispose of the information they gather.

Some City-provided services do not require the collection of PII. For example, no personal information is required to carry out such services as trash collection, street sweeping, snow plowing, and the cleaning and maintenance of City parks.

Storage of PII

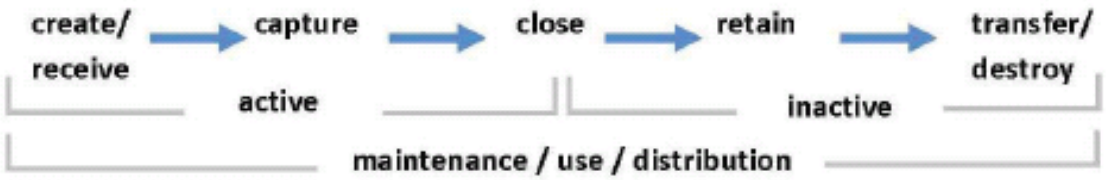
Personal data collected by City agencies is stored using a variety of methods depending on whether the information is electronic in nature or paper based. Electronic data is maintained on hard drives, network folders, databases, internal applications, or cloud-hosted applications. Some applications have built-in functionality that interface with state and federal systems. Paper-based PII should be stored behind badged doors, in locked file cabinets, or in private locked offices.

Retention of PII

City agencies should retain PII records in accordance with the City's General Records Retentions Schedule, unless they are subject to federal and state requirements. The length of time that a record should be retained varies by type of record. Federal and state funded programs are governed by separate retention requirements. For example, applications for food, financial, and medical assistance follow a tiered system of retention by which the federal, then state and City agency retention policies must be met. The City's General Records Retention Schedule specifies varying lengths of time for the retention of different types of documents. The City's Records Management Policy and Procedures Manual specifies a default retention period of three years for documents that are not explicitly covered within the policy.

As shown in Figure 1, all City records follow a pre-defined path, known as a life-cycle, depending on the type of record. When information is submitted to an agency, the record is considered *created*. Once the information contained in the record is verified, the record moves to the *capture* phase, which gives a record an *active* status. Once a record is closed, it has no reference value, and has reached the end of its useful life, the record is either destroyed or transferred offsite if it is considered a permanent record. Examples of permanent records are adoption, death, and marriage certificates.

FIGURE 1. Life-cycle of a City Record



Source: Records Management Policy and Procedures Manual, page 9.

Public Awareness of the City's Intended Use of PII

When individuals provide information of any kind to the City, they may wonder how the City will use that information and whether or not it will be secure in the City's possession. As identity theft and cyber-security threats have become all too common, these concerns are quite valid. The City has a Privacy and Security Policy, which is accessible to the public through the Denvergov.org website. The policy specifies what types of PII the City collects and makes clear that the City will not reveal any PII collected to third parties unless legally required to do so.

A link to the policy is located at the bottom of the Denvergov.org web page, as well as at the bottom of all pages that link to the main webpage. Most pages on the website have more content than can be displayed at once on a computer screen, so users must scroll to the bottom of the webpage to see the link to the Privacy and Security Policy. The link itself is displayed at the bottom of the page, along with the website copyright date and links to the City's jobs page, terms-of-use disclaimer, and the City's Colorado Open Records Act policy. Once the Privacy and Security policy is accessed users must once again navigate to the bottom of the policy before a statement on the City's handling of private information is displayed. Figure 2 is a screen capture of the homepage highlighting the location of the link to the privacy policy.

FIGURE 2. City and County of Denver Website Homepage

Source: www.denvergov.org.

Instances Where PII May Leave the City's Possession

Although the City safeguards PII pursuant to its Privacy and Security Policy, certain circumstances require the City to share PII with outside entities, including through requests made under the Colorado Open Records Act and for certain programs that operate using state or federal funds, such as Medicaid.

Colorado Open Records Act

The City's Privacy and Security Policy briefly explains how the City secures the information that an individual submits through a web form. The policy states that PII provided to the City in this way will not be made public. However, the City is subject to the provisions of the Colorado Open Records Act (CORA), which allows disclosure of some information to the public. Specifically, the Act states that autopsy reports are public records, but that any data maintained by a criminal justice department is not a public record. Entities that might request records under CORA include newspaper organizations, research institutions, businesses, other states, and political organizations. Members of the general public may also be interested in obtaining information within records that are accessible under CORA.

The following bullets provide examples of the types of requests that may be made of the City:

- Media Requests—Reporters may request that the City search employee emails for references to a topic on which they are reporting, such as "Black Lives Matter" or "homelessness."
- Bidding Requests—Contractors who bid on but do not win contracts to perform work on certain City projects may request the records of the other bidding contractors' proposals.
- Pre-Litigation Requests—Individuals or lawyers wanting information to evaluate a claim that may be brought against the City may request records with relevant information.
- 311 Requests—Individuals with a particular interest in the delivery of certain City services may request records about the provision of services, such as the number of pothole repair cases the City has received.[1]

While information can be requested through the CORA process, Colorado law recognizes many types of information that must remain closed to public inspection. For example, various types of PII such as social security numbers, home phone numbers or home addresses, as well as medical or mental health data is exempt from release to the public. CORA also closes other categories of public record from inspection, such as proprietary information.

Information Sharing with the State and Federal Government

In addition to data that may be released through a CORA request, some City agencies share PII with the federal government or the State of Colorado due to a shared system or funding relationship. For example, the Office of the Medical Examiner runs fingerprints of deceased individuals through a database that is maintained by the Federal Bureau of Investigation. Certain City services are federally funded, such as the Low-Income Energy Assistance Program, which provides assistance with winter home heating expenses and is administered locally by Denver Human Services. Residents are directed to provide information and an application to the department in their respective county. Applications are entered into a state system that interfaces with a federal system.

Data Classification and Handling Policy

To supplement the guidance found in CORA and the City's Records Management Policy and Procedures Manual, the City's Technology Services department created a Data Classification and Handling Policy, to which all City agencies are subject. The Data Classification and Handling Policy provides guidance to City agencies for assessing the sensitivity of the data they collect and how to handle different types appropriately. Data classification is the process by which different categories of data are assigned a value based on their degree of sensitivity. The intention of classifying data is to define whether or not authorization and identification is required, and whether the owner of the data must approve an information request.

The policy provides four classifications: (1) Public, (2) Reserved, (3) Confidential, and (4) Regulated. Regulated data, such as a social security number, has the strictest requirements and must not be released without notifying the City's Information Security Manager. Once data is classified, it must be protected by technical controls, which further define how assets, such as PII, are to be stored, transmitted, and destroyed. These controls vary for each classification. Finally, the policy defines the roles and responsibilities of entities directly involved with the data,

[1] 311 is a call center for citizens that provides residents with information that is helpful in navigating the City services.

including the owner, custodian, and Information Security Manager. For example, the owner ensures the asset is labeled appropriately to determine how to classify the data.

Identity Theft Is a Significant Threat to the Safety of PII

PII that is not publicly accessible must be safeguarded from both internal and external threats. One of the biggest threats to personal data is identity theft, which can occur when sensitive data is disclosed to unauthorized individuals or entities. Once data is stolen, it is used primarily for monetary gain. For example, a thief may use a stolen identity to obtain a credit card, commit tax or employment fraud, steal someone else's health insurance information, or reap social security benefits, to name just a few. Figure 3 gives three real-world examples of how identity theft may be perpetrated and the negative consequences for individuals and institutions.

FIGURE 3. Negative Consequences of Identity Theft

Children are increasingly becoming targets for identity theft because they do not have an existing credit history and it is unlikely that parents are requesting and monitoring their children's annual credit report. This makes children appealing targets to an individual who wants a new identity with which to perpetrate identity theft. Other targeted groups include college students, active-duty military, veterans, and seniors. Prisoners are also increasingly being targeted for identity theft to file fraudulent tax returns and to obtain credit.

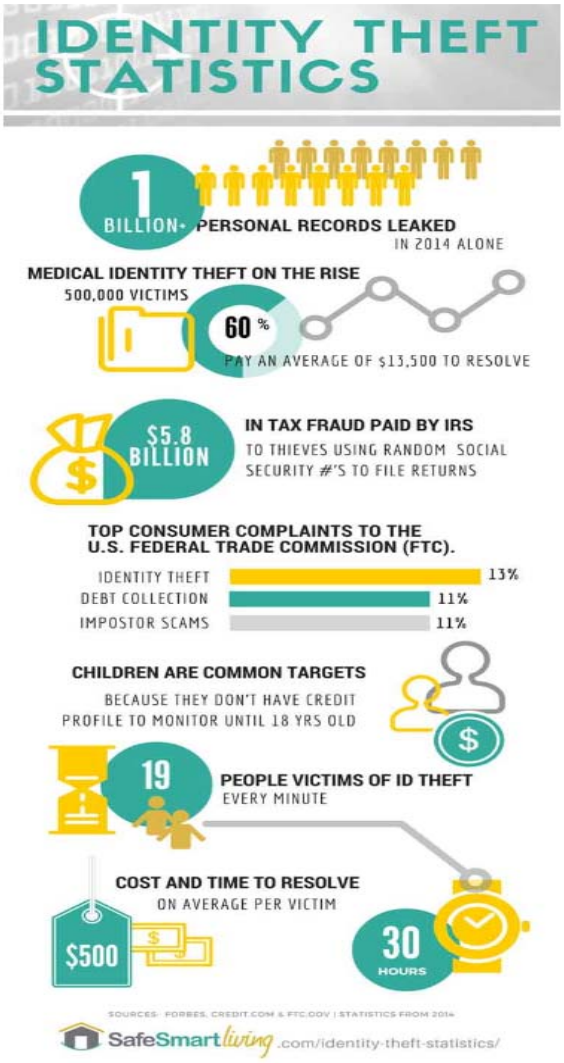
Potential Costs from Identity Theft

Victims of identity theft spend significant sums of money and hours of time recovering their identity and unwinding the damage done by the theft. Prisoners who fall victim to identity theft resulting in a fraudulent credit history are faced with an additional "obstacle to re-integrating with society by securing employment, housing, and access to credit."[2] Frequently, identify theft victims must pay late fees and penalties, higher credit card and lending interest rates, legal fees, and for credit monitoring services. Additionally, the victim may spend time filing reports, calling banks and credit card companies, and working with law enforcement. Victims often struggle to obtain financing and must try to clear their name with creditors and collection agencies, which seek to collect on debts the victims did not personally incur. On average, victims of identity theft estimate that they spent $500 and 30 hours resolving the problems encountered as a result of the identity theft, as shown in Figure 4. Colorado is ranked 13th for identify theft in 2013 according to a Federal Trade Commission report released in February 2014, with 4,195 complaints, or nearly 80 complaints per 100,000 people.[3]

[2] "Prisoners Vulnerable to Identity Theft," accessed on September 21, 2016, http://www.identityguard.com/identity-theft-resources/articles/prisoners-vulnerable-to-identity-theft/#.

[3] "Consumer Sentinel Network Data Book," *Federal Trade Commission*, (February 2014): page 27, https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-january-december-2013/sentinel-cy2013.pdf.

FIGURE 4. U.S. Identity Theft Statistics



Source: http://www.safesmartliving.com/identity-theft-statistics/?hlst=identity+theft+statistic

SCOPE

The audit evaluated current practices for the use and safeguarding of personally identifiable information (PII) by City agencies that gather this data. Medical information and credit card data PII categories were excluded from the scope of this audit since they are protected under the federal Health Insurance Portability and Accountability Act (HIPAA) and the Payment Card Industry (PCI) data security standards, respectively. Additionally, the Department of Safety was not included in the scope of this audit since information obtained thereby is covered under Criminal Justice Information Services (CJIS) security policy.

OBJECTIVE

The audit objective was to assess the effectiveness of the City's controls in place to safeguard PII. The audit objective included reviewing documented policies and procedures, employee training, public awareness, and protection of applications and networks as they relate to PII.

METHODOLOGY

We applied various methodologies during the audit process to gather and analyze information pertinent to the audit scope and to assist with developing and testing the audit objectives. The methodologies included the following:

- Assessing other cities' approaches to safeguarding PII
- Reviewing and assessing shared folders on the City network for evidence of unprotected PII with tools such as Varonis DatAdvantage and Active Directory Users and Computers
- Interviewing key personnel from several agencies to obtain contextual information about the collection and safeguarding of PII
- Reviewing and assessing agency policies, procedures, and training materials regarding the collection and protection of PII
- Assessing the effectiveness of the City's training on PII, including reviewing data collected from users that participated in the training
- Analyzing forms from selected agencies that collect PII to determine if a disclosure statement was included to notify the public how their PII would be safeguarded
- Consulting best practices established by sources such as the National Institute of Standards and Technology (NIST), Title 6 of the Colorado Revised Statutes, and the European Union's General Data Protection Regulation
- Reviewing the General Services Records Management Policy and Procedures Manual, and the General Records Retention Schedule
- Reviewing key Technology Services policies and procedures, including the Data Classification and Handling Policy, the Information Technology Acceptable Use Policy and Procedure, and City and County of Denver Website Privacy and Security Policy

- Observing the process for collecting, storing, and disposing of PII within several recreation centers
- Utilizing tools such as Barracuda Networks to verify encryption methods for securing external email transmissions and ServiceNow to verify that change requests exist for computers pending installation of encryption software

FINDING

The City Should Establish a Strategic Framework to Better Protect Personally Identifiable Information

Personally Identifiable Information, or PII, is information that uniquely identifies a person. As a collector of PII, the City and County of Denver (City) must have appropriate controls in place to protect that data from exposure or theft. In the process of assessing how the City is safeguarding PII, auditors uncovered two sources of unsecured sensitive personal data. We determined that this breakdown in controls is likely attributable to outdated policies and inconsistent practices regarding the management of PII. Accordingly, the City needs to establish a comprehensive strategy for managing PII from collection through disposal. However, to do so, we identified the need to compile a comprehensive inventory of PII, enforce employee training on the topic, and enhance transparency regarding how personal data is collected and handled.

Audit Uncovered Unsecured Network Folders and Hard Copy Data Containing PII

In assessing the effectiveness of the City's controls surrounding the protection of PII, we discovered a significant breakdown in the control structure, evidenced by thousands of pieces of unsecured, sensitive personally identifiable information. Most of this PII was contained in unsecured folders on the City's shared computer network, but other sources were found in hard copy awaiting destruction.

Unsecured Network Folders—During our testing, we came across and were able to open multiple folders on the City's shared network containing sensitive PII for employees as well as their dependents and beneficiaries. Specifically, these folders contained different types of PII, including fingerprints, social security numbers, bank account numbers, bank routing numbers, disciplinary actions, and information about children, spouses, or other beneficiaries' private information. In addition, one folder contained a database with 2,400 former employees' records, including date of birth and social security numbers.

It appeared upon discovery that the files containing this sensitive personal information were stored in folders that could have been accessed by anyone in the City with the appropriate credentials to access the computer network. To confirm that these folders were unsecured, the audit team used Varonis DatAdvantage, a security software tool that analyzes access rights and relationships within groups related to network files. This analysis confirmed that the files were indeed unsecured. Accordingly, all City employees who are members of a common access control list—approximately 10,000 employees—had read access to these folders, which opens up the possibility that these files may have been viewed by unintended users. However, we found no evidence that this type of unintended viewing occurred.

Unsecured Hard Copy Data—Additionally, we found an instance where hard copy PII that was waiting to be disposed of was not stored in a secure location. The data was located in a public area in a box file without a lid. Documents containing PII—including driver's license numbers, social security numbers, and full legal names—were stored in this unsecure manner.

Access to Unsecured PII Was Remediated

After discovering this unsecured PII, we promptly notified key City officials, including the Mayor, who immediately took action. Technology Services, the City's Information Technology and Security Department, subsequently secured access to the files containing this information; as such, the information is no longer available to all employees with network access. Although the City was responsive to these revelations of unprotected sensitive PII, remediation does not provide assurance that all such potential instances have been identified. Even though City management was informed about unsecured hard copy data, we have no evidence that this was addressed. More broadly, these instances underscore the need for improvements to the City's controls surrounding the handling of PII. As noted in the Introduction and Background section of this report, the City has established policies that provide guidelines and governance tactics for data and information assets. However, without proper dissemination and monitoring of compliance, breakdowns can occur. In the following sections, we explore why such a breakdown may have occurred.

Outdated Policy and Inconsistent Practices Highlight the Need for Citywide Strategy for PII

Audit work revealed that the City does not have an overarching strategy addressing the proper handling of sensitive information, such as PII. During the course of the audit, Technology Services management told the audit team that they are in the process of creating a policy that would leverage existing Colorado state law regarding the collection and safeguarding of PII. However, Technology Services did not produce any documentation evidencing this work and, as of the publication of this report, such a policy is still in progress.

Although the City lacks an overarching strategy for proper handling of PII, the City does have policies that focus on relevant areas, including the Data Classification and Handling Policy and the Records Management Policy.[4] However, some of these policies have not been regularly revised or approved by City leadership. Further, communication regarding the existence of these policies has not been consistent across all City agencies, in some cases instigating the creation of separate policies by individual agencies and ultimately leading to inconsistent handling of PII. The issues surrounding updates, approval, and communication are outlined in greater detail below:

- **Records Management Policy and Procedures Manual**—The purpose of this policy is to provide guidance in the storage, retention, and destruction practices used to manage official records and files. Additionally, the policy establishes processes to secure and regulate access to records and files and retain them based on historical value. While this policy has not been updated since July 23, 2012, and was approved by a former City Records Manager, the General Records Retention Schedule has been kept up to date. This policy does not include specific guidance on PII incident response, data breach notification, or sanitizing hardware prior to disposal, all of which are established as best

[4] These policies are described in detail in the Introduction and Background section of this report.

practices in accordance with the National Institute for Standards and Technology (NIST) framework for managing PII (NIST framework).[5]

- **Data Classification and Handling Policy**—The purpose of this policy is to ensure that all agencies, employees, and contractors that conduct business for the City appropriately define the value of their information assets and that defined safeguards are implemented to protect these assets, including PII. This policy has not been updated since September 6, 2011, and was approved by the City's former Director of Enterprise Architecture, and the former Chief Information Officer. This policy does not include specifics on PII retention procedures, personnel awareness, training and education, or limiting the collection of PII to the minimum necessary, all of which are established as best practices in accordance with the NIST framework.

Disparate Handling of PII Citywide—After conducting interviews with relevant personnel in several City agencies that collect PII, we found that some agencies were unaware of relevant Citywide policies, including the Data Classification and Handling Policy and the Records Management Policy. Additionally, we found that some of these agencies rely instead on internally created policies that are not consistent with City requirements or industry standards. Specifically, many of these agency-created policies did not include procedures regarding employee training, retention and disposal, or transparency with individuals whose PII is being collected.

The City Needs To Establish a Comprehensive Framework for Consistent Management of PII Citywide

To prevent future instances of exposed PII and to promote continuity among City departments, the City needs a strategic framework for capturing, safeguarding, and disposing of PII. The most widely accepted framework for managing PII is known as Fair Information Practices (FIPs). FIPs are a set of recognized principles to address the privacy of information about individuals. FIPs are important because they provide the underlying policy for many laws addressing privacy and data protection matters. In fact, this widely accepted framework is central to the Federal Privacy Act of 1974 and is reflected in the laws of many federal agencies, states, and even other countries. For instance, the U.S. Department of Homeland Security (DHS) uses FIPs as the foundation of all its privacy policy and the principles must be considered whenever any DHS activity involves the collection of PII. In other words, any time DHS collects PII, they have to follow FIPs.[6]

FIPs collectively include eight principles, formally established by the Organization for Economic Co-operation and Development (OECD).[7] These principles were first included in privacy

[5] National Institute of Standards and Technology Special Publication 800-122, "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)," April 2010.

[6] Other uses of FIPs in the federal government include the U.S. Department of Health and Human Services, U.S. Department of Commerce, Federal Trade Commission, National Strategy for Trusted Identities in Cyberspace, and National Science and Technology Council.

[7] The mission of the Organization for Economic Co-operation and Development, or OECD, is to promote policies that will improve the economic and social well-being of people around the world. Established in 1961, the OECD has 35 member countries, including the United States, and provides a forum where governments can work toward solutions to common problems. Recognizing the privacy challenges facing governments with the development of automatic data processing, the

guidelines created by the OECD in 1980—the first internationally agreed-upon set of privacy principles—and were subsequently updated in 2013. The eight principles are as follows:

- **Openness**—There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
- **Individual Participation**—An individual should have the right: a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to them; b) to have communicated to them, data relating to them within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to them; c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and d) to challenge data relating to them and, if the challenge is successful to have the data erased, rectified, completed or amended.
- **Purpose Specification**—The purposes for which personal data are collected should be specified no later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
- **Collection Limitation**—There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
- **Use Limitation**—Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with [the Purpose Specification principle] except: a) with the consent of the data subject; or b) by the authority of law.
- **Data Quality**—Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
- **Security Safeguards**—Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.
- **Accountability**—A data controller should be accountable for complying with measures which give effect to the principles stated above.

There is broad international agreement on the substance of FIPs and their importance in establishing privacy programs. According to the National Institute of Standards and Technology (NIST), "To establish a comprehensive privacy program that addresses the range of privacy issues that organizations may face, organizations should take steps to establish policies and procedures that address all of the Fair Information Practices."[8]

OECD developed Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. These guidelines were updated in 2013. http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

[8] "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)", Special Publication 800-122, National Institute of Standards and Technology, U.S. Department of Commerce (April 2010).

Accordingly, we recommend that the Mayor's Office work with Technology Services to develop a City strategy, reinforced by updated Citywide policies, to incorporate the eight fair information practice principles. Furthermore, these policies should be periodically reviewed and updated, annually disseminated, and approved by City leadership to ensure that they align with City strategy.

In order to establish and implement a robust strategy for handling PII, the City will need to develop an inventory of all PII gathered Citywide and train people on the elements of the strategy itself. Additionally, to effectuate transparency of the process, the City should undertake public awareness efforts.

The City Needs to Define and Compile a Comprehensive Inventory of PII

As part of our audit work, we sought to determine some of the collection points of PII throughout the City, along with the variety of PII that is being collected. Although the City does not have a comprehensive inventory of PII collected Citywide, we learned that the City's Risk Management Office (Risk Management) recently compiled a relatively thorough PII inventory as part of an application process for updating the City's liability insurance. In 2015, Risk Management distributed a survey to all agencies to gain an understanding of when PII is collected. Based on survey feedback, they developed a list of agencies that collect this data. For each agency included on the list, they indicated what types of PII were being collected by that agency.

To determine the completeness of this list, we conducted our own interviews of personnel from agencies on the list and compared our results to the list developed by Risk Management. We determined that three of the agencies did not have complete entries capturing all of the types of PII they collect. One agency's entry did not include a financial assistance program for which it collects PII, another agency's entry did not include an application it uses to collect PII, and a third agency's entry was missing specific data on what type of PII is collected.

Maintaining a complete inventory of PII collected by the City is a crucial starting point to protecting data that is collected throughout the City. A complete inventory should include information about the amount of data collected, classification of PII, data retention period, the location and format of the stored PII (for example, shared network folder, database, filing cabinet, or off-site storage), and how access is currently restricted. This information is necessary in order to implement the appropriate measures to monitor and safeguard the data.

NIST recommends that organizations identify all PII residing within their organization. Furthermore, the NIST framework notes that the access to and location of PII is an important consideration; if PII is accessed more frequently or stored on laptops or removable media, the organization should assign a higher risk level.[9] Therefore, we recommend that the Mayor's Office work with Technology Services to develop a universal definition of PII and create an annually updated inventory of where PII is collected and stored.

City's PII Training Course Is Not Enforced

The City requires an annual training course to City employees called Securing the Human provided through the SANS Institute, which offers information security training, certification, and research. The training is administered by Technology Services and provides coverage of general concepts related to safeguarding and protecting PII. Specifically, the training includes multiple

[9] Ibid., page 3-3.

videos that explain the importance of protecting information that can identify a person. However, while the training does appear to provide a valuable message, we found that the training was not completed by nearly 40 percent of City employees. When auditors asked about the reason for this low completion rate, we determined that completion of the training is not enforced. This is true both for employees and contingent workers, who also have access to the City network.

NIST recommends that organizations establish a training plan related to PII to reduce the possibility that PII will be accessed, used, or disclosed inappropriately. Additionally, all individuals that have been granted access to PII should receive appropriate training and, where applicable, specific role-based training.[10]

Accordingly, we recommend that the Mayor's Office work with Technology Services to establish training requirements for City employees handling PII. Specifically, the training should define roles and responsibilities for training; training prerequisites for receiving access to PII; and training frequency and refresher training requirements. To reduce the possibility that PII will be accessed, viewed, or disclosed inappropriately, all individuals who have been granted access to PII should receive appropriate training and, where applicable, specific role-based training.

The City's Comprehensive PII Strategy Should Include Public Awareness Efforts and Specify Collection Requirements

As mentioned previously, several of the agencies we selected for testing have disclosure statements on forms or applications that require PII. The disclosure statements state that they inform the public how their PII is handled, stored, and collected. After reviewing a sample of disclosure statements, however, we determined that three out of the six agencies tested do not inform the public on how their PII is safeguarded. The other three agencies do have disclosure statements that mention privacy concerns; however, they also do not explain how the data is safeguarded. Furthermore, the way in which the City's Privacy and Security Policy is displayed on the Denvergov.org website is rather discreet, as compared to the more prominent display of the State of Colorado's Privacy Statement that auditors observed on the Colorado.gov website.

Effective disclosure statements inform the public about activities that impact information privacy. According to the NIST framework, public disclosure information should explain how PII is collected, used, shared, safeguarded, maintained, and disposed of. Accordingly, the overarching PII strategy should include requirements for informing the public on use and safeguarding of PII.

The City's Lack of a Strategy for Managing PII Has Several Negative Effects

Citywide PII must be protected to ensure an individual's identity is safe and secure. Without a strong strategy in place to protect PII, individuals can be at risk for identity theft. The findings in this report highlight the fragmented approach the City has in place to safeguard PII and identify the need for a strong strategic plan in order to prevent the risk of identity theft to an individual. The following risks can ultimately lead to exposure of an individual's identity, which in turn could result in identity theft.

- A lack of policies and procedures could lead to the mishandling, loss, or theft of PII.

[10] The OECD Privacy Framework (2013), page 91.

- Disclosure statements that fail to inform the public on how their data is being collected limits transparency and restricts public awareness of how their PII is being safeguarded.
- Without a comprehensive and detailed inventory of PII, the City is at risk for potential unauthorized access to an individual's PII. Additionally, the City may not have all of the information required to perform an adequate risk assessment, develop adequate security controls, and ensure compliance with records retention policies.
- PII stored on unprotected shared drives throughout the City's network and unsecure hard copy PII can lead to unauthorized access. In the event that the data were to be misused, the City could be liable for legal fees and fines as well as suffer reputational damage.

RECOMMENDATIONS

1.1 **Documented Guidance** - The Mayor's office needs to provide documented guidance based on NIST and FIPS standards that is updated and disseminated annually, and focuses on safeguarding Personally Identifiable Information (PII) to ensure continuity and a basic level of data protection among agencies. This guidance should be communicated through policy or executive order and include the following:

- Definition of PII
- Access rules for PII within a system
- Incident response and data breach notification
- Retention schedule and procedures
- Limits for collection, disclosure, sharing and the use of PII
- Consequences for failure to follow privacy rules of behavior
- Privacy-specific safeguards
- Requirements for informing the public on use and safeguarding of PII
- Review of the City's holdings, and destruction if they are not relevant
- Disposal in accordance with litigation holds and the City's General Records Retention Schedule
- Specify a redaction or encryption procedure
- Ensure hardware has been properly sanitized prior to disposal
- Awareness, Training & Education

Auditee Response: Agree, Implementation Date – March 31, 2017

We have convened an Information Governance Committee that is currently addressing PII policies and procedures as part of its mission. Key stakeholders will work within the committee and with City agencies to establish a strategic framework for managing PII policies, procedures, and training. The results will be communicated through policies or executive order as appropriate.

1.2 **Policy Review and Signoff** - If existing policies are incorporated as part of the overall strategy, the Mayor's Office should ensure that they are signed by current management, reviewed annually and disseminated/publicized.

Auditee Response: Agree, Implementation Date – March 31, 2017

We will ensure our policies are signed by current officials as appropriate and that they will be reviewed annually with appropriate notification.

1.3 **Inventory of PII** - The Technology Services governance team or another team, as designated by the mayor's office, should collect and maintain a complete and detailed inventory of PII.

Auditee Response: Agree, Implementation Date – March 31, 2017

Technology Services will work with City agencies to gather and maintain a complete and detailed inventory of PII.

1.4 **Access Rights** - Technology Services should complete their evaluation of network shared folders and the implementation of individual and group access rights and address any findings to ensure that network shares are configured appropriately to support limited access to PII.

Auditee Response: Agree, Implementation Date – First agency by March 31, 2017 with the rest by December 31, 2017

We initiated a project to carefully examine how access permissions to shared folders are currently configured and to develop a strategy to ensure network shares are configured appropriately to limit access to PII. Overall, there are approximately 300 root shares containing 150 TB of data across 100 million files throughout the City. As each agency has varying needs, they will be remediated one by one.

1.5 **Tools to Safeguard Data** - Technology Services should ensure that the data owners for each agency have the necessary tools or information to fulfill their role in safeguarding data. The tools or information should enable the data owners to review access to network shares that contain PII.

Auditee Response: Agree, Implementation Date – March 31, 2017

Technology Services is currently using two different tools for file analytics and is in the process of evaluating additional solutions with more features including compliance and alerting.

1.6 **Roles and Responsibilities** - Technology Services should define roles and responsibilities for administering annual training for PII; employee training prerequisites for receiving access to PII; and employee training periodicity and refresher training requirements.

Auditee Response: Agree, Implementation Date – March 31, 2017

Technology Services has invested in a security awareness training tool that includes specific education on PII that will be integrated into the existing online training software utilized by the City's Office of Human Resources (OHR). TS will define roles and responsibilities for administering the security awareness training, employee training frequency, and refresher training requirements. There is also a communication plan in progress to increase the visibility of the training. In addition, key reporting metrics will be more effectively utilized to enforce the completion of training.

APPENDIX

If you are interested in learning more about how to protect yourself or your family or if you believe you may have been a victim of identity theft the following resources may be of assistance.

Resources for individuals:

1. Stop Fraud Colorado (Colorado Attorney General's Office) – Fraud Center
   http://www.stopfraudcolorado.gov/fraud-center

   Contains articles on a wide variety of topics, including tips for protecting your own information, a list of steps to take if you have been a victim of identity theft and special interest articles for seniors and Military Members. The site also includes information presented in Spanish.

2. Stop Fraud Colorado (Colorado Attorney General's Office) Identity Theft Resources
   http://www.stopfraudcolorado.gov/fraud-center/identity-theft/identity-theft-resources

   Provides links to Federal Trade Commission (FTC), Department of Justice, Colorado Bureau of Investigations – Identity Theft Hotline, Credit Reporting Agencies, and Publications and Handbooks.

   The Publications and Handbooks linked to this page include:

   a. Immediate Steps to Repair Identity Theft – FTC
      https://www.identitytheft.gov/#what-to-do-right-away

   b. Safeguarding Your Childs Future- FTC
      https://www.consumer.ftc.gov/articles/0040-child-identity-theft

   Both of these publications are available in Spanish.

3. Colorado Bureau of Investigation, Department of Public Safety –Identity Theft/Cyber Crimes https://www.colorado.gov/pacific/cbi/identity-theftcyber-crimes

   Identity Theft topics include identity theft, fraud and cyber-crimes prevention, types of identity theft and fraud, and crime unit contacts.

4. Get Your Free Credit Report, Federal Trade Commission, https://www.ftc.gov

If you are a business owner and would like to know more about protecting your business or the personal information of your customers and employees, the following resources may be of assistance.

Resources for businesses:

1. Protecting Personal Information: A Guide For Business,
   http://www.stopfraudcolorado.gov/sites/default/files/bus69-protecting-personal-information-guide-business_0.pdf

2. Business Identity Theft Resource Guide: A Guide to Protecting Your Business and Recovering from Business Identity Theft, http://www.stopfraudcolorado.gov/sites/default/files/BITguide.pdf

AGENCY RESPONSE

Office of Mayor Michael B. Hancock

City and County Building
1437 Bannock St, Room 350
Denver, CO 80202-5390
p: 720.865.9090
denvergov.org/mayor

DENVER
THE MILE HIGH CITY

October 28, 2016

Auditor Timothy O'Brien, CPA
Office of the Auditor
City and County of Denver
201 West Colfax Avenue, Dept. 705
Denver, Colorado 80202

Dear Mr. O'Brien,

The Office of the Auditor has conducted a performance audit of Personally Identifiable Information.

This memorandum provides a written response for each reportable condition noted in the Auditor's Report final draft that was sent to us on October 17, 2016. This response complies with Section 20-276 (c) of the Denver Revised Municipal Code (D.R.M.C.).

AUDIT FINDING 1
The City should establish a strategic framework to better protect personally identifiable information

RECOMMENDATION 1.1
The Mayor's office needs to provide documented guidance based on NIST and FIPS standards that is updated and disseminated annually, and focuses on safeguarding Personally Identifiable Information (PII) to ensure continuity and a basic level of data protection among agencies. This guidance should be communicated through policy or executive order and include the following:

- Definition of PII
- Access rules for PII within a system
- Incident response and data breach notification
- Retention schedule and procedures
- Limits for collection, disclosure, sharing and the use of PII
- Consequences for failure to follow privacy rules of behavior
- Privacy-specific safeguards
- Requirements for informing the public on use and safeguarding of PII
- Review of the City's holdings, and destruction if they are not relevant
- Disposal in accordance with litigation holds and the City's General Records Retention Schedule
- Specify a redaction or encryption procedure
- Ensure hardware has been properly sanitized prior to disposal
- Awareness, Training & Education

Agree or Disagree with Recommendation	Target date to complete implementation activities (Generally expected within 60 to 90 days)	Name and phone number of specific point of contact for implementation
Agree	March 31, 2017	David Edinger 720-865-9033

Narrative for Recommendation 1.1
We have convened an Information Governance Committee that is currently addressing PII policies and procedures as part of its mission. Key stakeholders will work within the committee and with City agencies to establish a strategic framework for managing PII policies, procedures, and training. The results will be communicated through policies or executive order as appropriate.

RECOMMENDATION 1.2
If existing policies are incorporated as part of the overall strategy, the Mayor's Office should ensure that they are signed by current management, reviewed annually and disseminated/publicized.

Agree or Disagree with Recommendation	Target date to complete implementation activities (Generally expected within 60 to 90 days)	Name and phone number of specific point of contact for implementation
Agree	March 31, 2017	David Edinger 720-865-9033

Narrative for Recommendation 1.2
We will ensure our policies are signed by current officials as appropriate and that they will be reviewed annually with appropriate notification.

RECOMMENDATION 1.3
The Technology Services governance team or another team, as designated by the mayor's office, should collect and maintain a complete and detailed inventory of PII.

Agree or Disagree with Recommendation	Target date to complete implementation activities (Generally expected within 60 to 90 days)	Name and phone number of specific point of contact for implementation
Agree	March 31, 2017	Tricia R. Scherer 720-913-4869

Narrative for Recommendation 1.3
Technology Services will work with City agencies to gather and maintain a complete and detailed inventory of PII.

RECOMMENDATION 1.4 Technology Services should complete their evaluation of network shared folders and the implementation of individual and group access rights and address any findings to ensure that network shares are configured appropriately to support limited access to PII.		
Agree or Disagree with Recommendation	**Target date to complete implementation activities (Generally expected within 60 to 90 days)**	**Name and phone number of specific point of contact for implementation**
Agree	First agency by March 31, 2017 with the rest by December 31, 2017	Tricia R. Scherer 720-913-4869

Narrative for Recommendation 1.4
We initiated a project to carefully examine how access permissions to shared folders are currently configured and to develop a strategy to ensure network shares are configured appropriately to limit access to PII. Overall, there are approximately 300 root shares containing 150 TB of data across 100 million files throughout the City. As each agency has varying needs, they will be remediated one by one.

RECOMMENDATION 1.5 Technology Services should ensure that the data owners for each agency have the necessary tools or information to fulfill their role in safeguarding data. The tools or information should enable the data owners to review access to network shares that contain PII.		
Agree or Disagree with Recommendation	**Target date to complete implementation activities (Generally expected within 60 to 90 days)**	**Name and phone number of specific point of contact for implementation**
Agree	March 31, 2017	Tricia R. Scherer 720-913-4869

Narrative for Recommendation 1.5
Technology Services is currently using two different tools for file analytics and is in the process of evaluating additional solutions with more features including compliance and alerting.

RECOMMENDATION 1.6 Technology Services should define roles and responsibilities for administering annual training for PII; employee training prerequisites for receiving access to PII; and employee training periodicity and refresher training requirements.		
Agree or Disagree with Recommendation	**Target date to complete implementation activities (Generally expected within 60 to 90 days)**	**Name and phone number of specific point of contact for implementation**
Agree	March 31, 2017	Tricia R. Scherer 720-913-4869

Narrative for Recommendation 1.6
Technology Services has invested in a security awareness training tool that includes specific education on PII that will be integrated into the existing online training software utilized by the City's Office of Human Resources (OHR). TS will define roles and responsibilities for administering the security awareness training, employee training frequency, and refresher training requirements. There is also a communication plan in progress to increase the visibility of the training. In addition, key reporting metrics will be more effectively utilized to enforce the completion of training.

Please contact Tricia R. Scherer at 720-913-4869 with any questions.

Sincerely,

David P. Edinger
Chief Performance Officer

Scott Cardenas
Chief Information Officer

cc: Valerie Walling, Deputy Auditor, CPA, CMC
Shannon Kuhn, Information Technology Audit Supervisor, CISA
Chris Todd, Chief Technology Officer
Stephen E. Coury, Chief Information Security Officer
Tricia R. Scherer, IT Governance Manager