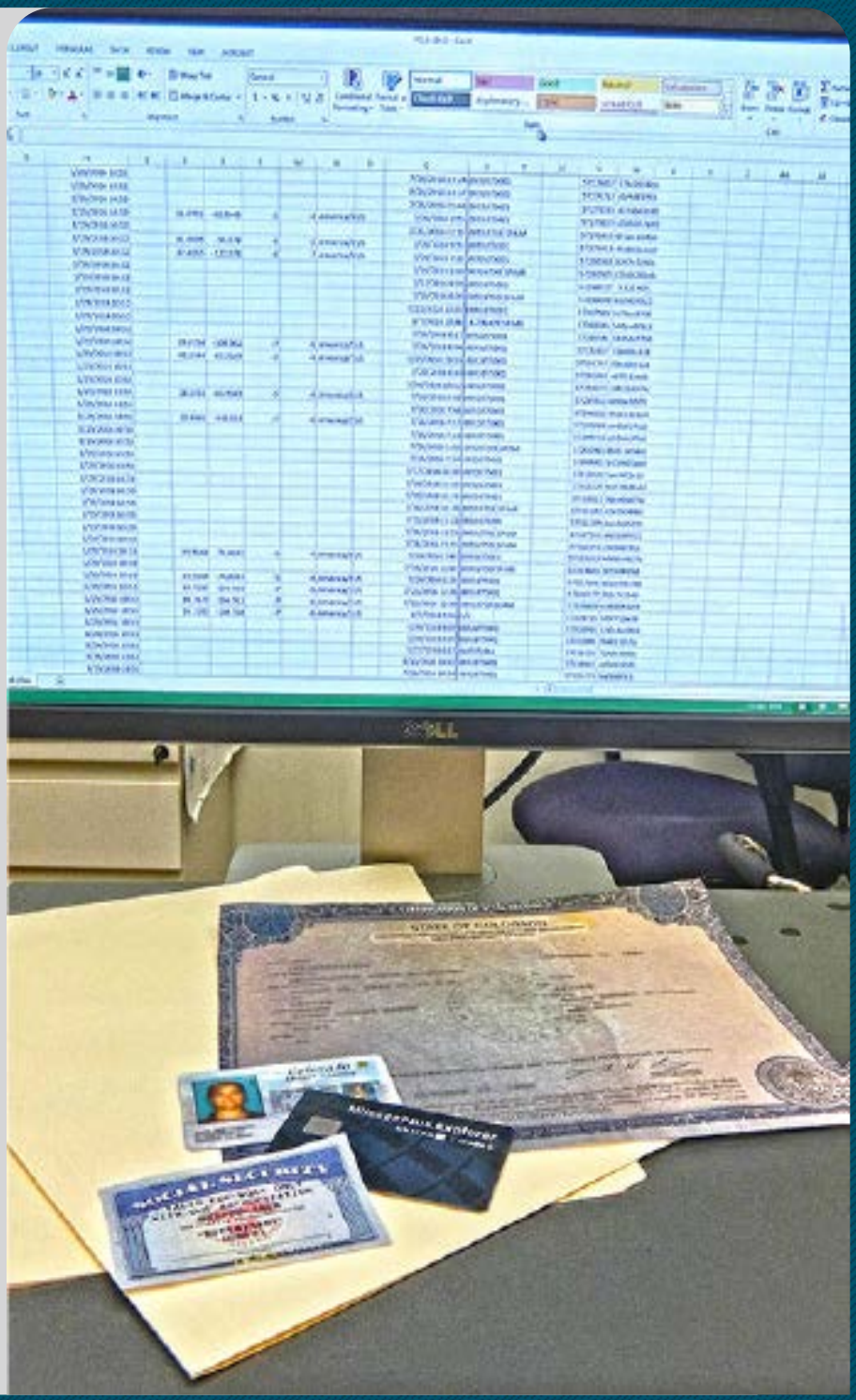
FOLLOW-UP REPORT
Citywide
Personally Identifiable Information Audit
July 2018



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 and contractors 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.

The Audit Committee is chaired by the Auditor and consists of seven members. The Audit Committee assists the Auditor in his oversight responsibilities regarding the integrity of the City's finances and operations, including the reliability 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

Timothy M. O'Brien, CPA, Auditor
Valerie Walling, CPA, CMC®, Deputy Auditor
Heidi O'Neil, CPA, CGMA, Director of Financial Audits
Kevin Sear, CPA, CIA, CISA, CFE, CGMA, Audit Manager

Audit Team

Nick Jimroglou, CISA, Lead IT Auditor
Karin Doughty, CISA, Senior IT Auditor
Shannon Kuhn, CISA, 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
Audit report year: **2016**

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

July 5, 2018

Evan Dreyer, Deputy Chief of Staff
Mayor's Office
David Edinger, Chief Information Officer
Technology Services
Ray Sibley, Director of Risk Management
Denver Risk Management Office
City and County of Denver

Re: Audit Follow-Up Report

Dear Messrs. Dreyer, Edinger, and Sibley:

In keeping with generally accepted government auditing standards and the Audit Services Division's policy, as authorized by D.R.M.C. § 20-276, our Division has a responsibility to monitor and follow up on audit recommendations to ensure that audit findings are being addressed through appropriate corrective action and to aid us in planning future audits.

This report is our follow-up to the Personally Identifiable Information audit issued December 15, 2016. The audit made six recommendations, two to the Mayor's Office and four to Technology Services. Our review determined the Mayor's Office has partially implemented one recommendation and fully implemented another. Meanwhile, Risk Management addressed and fully implemented one of the Technology Services recommendations. Technology Services partially implemented the three remaining recommendations. Because the Mayor's Office and Technology Services' commendable efforts are still in progress, auditors determined that the risk associated with the audit team's initial findings has not been fully mitigated. As a result, the Division may revisit these risk areas in future audits to ensure that appropriate corrective action is taken.

For your reference, this report includes a highlights page that provides background and summary information on the original audit and the completed follow-up effort. Following the highlights page is a detailed implementation status update for each recommendation.

This concludes audit follow-up work related to this audit. I would like to express our sincere appreciation to you and to the Mayor's Office and Technology Services personnel who assisted us throughout the audit and follow-up process. If you have any questions, please feel free to contact me at 720-913-5000 or Kevin Sear, Internal Audit Manager, at 720-913-5068.

Denver Auditor's Office

Timothy M. O'Brien, CPA
Auditor

REPORT HIGHLIGHTS

Personally Identifiable Information

July 2018

Status

The Mayor's Office agreed with two recommendations we made in the December 2016 audit, and has fully implemented one and partially implemented another. Technology Services agreed with each of four recommendations. Our follow-up audit work revealed that Risk Management has implemented one and Technology Services partially implemented the three remaining recommendations.

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.

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.

Highlights from Original Audit

The audit found that the City did not have a strategic framework for protecting personally identifiable information (PII). Specific areas of concern included 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 offered several recommendations to mitigate these risks.

Findings at Follow-up

In 2016, the Information Governance Committee (IGC) was formed by the Mayor's Chief Performance Officer, Chief Information Officer, and Senior City Attorney to address city processes and procedures for data governance. The IGC developed and recommended a mayoral executive order. Executive Order 143, dated February 16, 2018, established the protected data privacy policy and authorized the IGC to provide guidance for the policy's implementation. These actions created the foundation for a comprehensive protected data program. In addition, Technology Services created and filled a Chief Data Protection Officer position to work with the IGC to address the audit recommendations. The IGC has established working groups to address a variety of topics including training, data mapping/data stewards, HIPAA, and Payment Card Industry (PCI) compliance. Finally, Risk Management enhanced its annual cyber exposure questionnaire to obtain a more complete inventory of PII and other sensitive data. Despite the progress that has been made, the Mayor's Office and Technology Services provided a revised date of June 30, 2019 to fully implement the remaining recommendations.

For a copy of this report, visit www.denvergov.org/auditor or contact the Auditor's Office at 720-913-5000.

Recommendations: Status of Implementation

Recommendation		Auditee Action	Status
FINDING: The City Should Establish a Strategic Framework to Better Protect Personally Identifiable Information			
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	In 2016, the Information Governance Committee (IGC) was formed by the Mayor's Chief Performance Officer, Chief Information Officer and Senior City Attorney to address city processes and procedures for data governance. As a result, an IGC working group developed and recommended a mayoral executive order. Executive Order 143, dated February 16, 2018, established the protected data privacy policy for the City and County of Denver, and authorized the Information Governance Committee (IGC) to provide guidance for the policy's implementation. The IGC established a charter, a process and a team collaboration site. The committee, which meets monthly, has established working groups for topics including training, and Payment Card Industry (PCI) activities. Finally, Technology Services created and filled a Chief Data Protection Officer position to work with the IGC to address all the items listed in the recommendation. The Mayor's Office provided a revised completion date of June 30, 2019.	**Partially Implemented** **Original target date for completion: March 31, 2017**

Recommendations: Status of Implementation

	Recommendation	Auditee Action	Status
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.	The Information Governance Committee's policies, standards, and procedures approval lifecycle includes steps for multiple approvals, publication, communication, and periodic reviews.	**Implemented**
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.	Risk Management incorporated additional data fields into its 2018 annual cyber exposure questionnaire and inventory to provide a more complete inventory of PII and other sensitive data. In addition, Technology Services has two different file analytics tools that can be used to perform searches and identify PII.	**Implemented**

Recommendations: Status of Implementation

	Recommendation	Auditee Action	Status
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.	Technology Services began a process to partner with agencies to remediate access to its file shares in accordance with role based access. The Chief Data Protection Officer has prepared a draft privacy program manual that includes a section on access control policies and procedures. Other efforts include the development of an Access Control Review Procedures and Desk Guide (draft). The guide explains that each agency under the Mayor will be required to identify at least one agency contact to review access to shared folders. Agencies will also be required to map the use and storage of personally identifiable information. Technology Services provided a revised implementation date of June 30, 2019.	**Partially Implemented** **Original target date for completion: December 31, 2017**
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.	Technology Services currently uses two different tools for file analytics. The Access Control Review Procedures and Desk Guide (draft) explains that each agency under the Mayor will be required to identify at least one agency contact that can assist with managing access requests for their agency. The Desk Guide introduces the agency contacts to one of the file analysis tools, explains key concepts, and offers training with the Chief Data Protection Officer to understand how to effectively review access to file shares. Technology Services provided a revised implementation date of June 30, 2019.	**Partially Implemented** **Original target date for completion: March 31, 2017**

Recommendations: Status of Implementation

	Recommendation	Auditee Action	Status
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.	The Information Governance Committee's (IGC) training working group has developed a training policy that defines roles and responsibilities and specifies that all employees/contingent workers complete cybersecurity and privacy training. The policy (final draft) also notes that additional training may be required depending upon specific job requirements. The required annual Cybersecurity Awareness training has been integrated into CityU which provides enhanced tracking and reporting, however mandatory privacy training has not yet been implemented. Technology Services implemented a communication plan in 2017 using employee bulletins and emails to increase the visibility of the cybersecurity training. Technology Services provided a revised implementation date of June 30, 2019.	**Partially Implemented** **Original target date for completion: March 31, 2017**

Conclusion

While the Mayor's Office implemented one recommendation made in the Personally Identifiable Information audit report and partially implemented another, much has been accomplished in the interim, including the formation of the Information Governance Committee (IGC), and the development and issuance of Executive Order 143, which established the protected data privacy policy. Meanwhile, Risk Management addressed and fully implemented one of the Technology Services recommendations by enhancing an existing questionnaire to obtain the required data. Technology Services partially implemented three additional recommendations. Notably, Technology Services (TS) created and filled a Chief Data Protection Officer position to work with the IGC to address the audit recommendations. TS has also integrated cybersecurity training into the City's training platform, and has made progress on developing draft copies of privacy documentation and policies. Despite the Mayor's Office and Technology Service's efforts, auditors determined that the risk associated with the audit team's initial findings has not been fully mitigated. As a result, the Audit Services Division may revisit these risk areas in future audits to ensure appropriate corrective action is taken.

On behalf of the citizens of the City and County of Denver, we thank staff and leadership from the Mayor's Office, Technology Services, and Department of Finance/Risk Management for their cooperation during our follow-up effort and their dedicated public service.