February 27, 2019

Performance Audit

Personal Identifiable Information (PII) Security on City Systems

Citywide

Report No. 18-103

CITY OF ALBUQUERQUE
OFFICE OF INTERNAL AUDIT

PERFORMANCE AUDIT REPORT
PERSONAL IDENTIFIABLE INFORMATION (PII)
SECURITY ON CITY SYSTEMS
CITYWIDE REPORT
REPORT NO. 18-103

TABLE OF CONTENTS PAGE NO.

City of Albuquerque - Office of Internal Audit

Personal Identifiable Information (PII) Security on City Systems

Performance Audit | February 27, 2019 | Audit #18-103

The purpose of the audit was to identify City systems storing Personal Identifiable Information (PII), and to determine if the information is secure.

Executive Summary

The increase in security breaches involving PII has contributed to the loss of millions of records over the past few years. Security breaches involving PII are harmful to both organizations and individuals. Organizational damages may include a loss of public trust, legal liability, or remediation costs. Individual damages may include identity theft, embarrassment, or blackmail.

Department of Technology & Innovation (DTI) does not maintain an active inventory of systems and devices that contain PII. The City also does not have comprehensive policies and procedures for classifying and safeguarding PII. In addition, individuals with access to the City's computer environment are not always trained on or aware of their responsibility to safeguard PII.

DTI can effectively manage PII security on City systems by:

- Maintaining an active inventory of systems and device containing PII,
- Ensuring policies and procedures and underlying controls for classifying and safeguarding PII at the department level are established, and
- Ensuring that employees with access to PII are trained on and aware of their responsibility to safeguard PII.

OIA identified 27,037 records containing high-risk PII in one of the three City systems tested. According to the 2018 Cost of Data Breach Study – Global Overview, performed by the Ponemon Institute LLC, the average cost per record breached is $148 per record. A breach of the 27,037 records would result in a cost of approximately $4 million to the City.

DTI agrees with the findings and recommendations.

Recommendations

DTI should:

- Review internal controls, develop processes, and assign responsibility to ensure that an active inventory of systems and devices containing PII is maintained.
- Review all City information systems to ensure that all PII is identified, classified, and safeguarded.
- Review identified PII and determine if it is relevant and necessary.
- Develop comprehensive policies and procedures for classifying and safeguarding PII.
- Review its current practices including IT functions maintained by City departments outside of DTI's main authority and develop citywide policies and procedures that address data breaches.
- Train City department staff on classifying and safeguarding PII.
- Communicate regularly with City departments to ensure that all individuals with access to the computer environment are trained on and aware of the City's policies and procedures on PII and their responsibility for safeguarding PII.

City of Albuquerque

Office of Internal Audit

February 27, 2019

Accountability in Government Oversight Committee
P.O. Box 1293
Albuquerque, New Mexico 87103

Audit: Personal Identifiable Information (PII) Security on City Systems
Citywide
Audit No. 18-103

FINAL

INTRODUCTION

The Office of Internal Audit (OIA) completed a citywide performance audit of Personal Identifiable Information (PII) Security on City of Albuquerque (City) Systems for the audit period encompassing fieldwork, from October 2, 2018 to January 23, 2019. This audit was included in OIA's fiscal year (FY) 2018 audit plan. Information pertaining to the audit objectives, scope, limitations and methodology can be found in **Appendix A**.

The increase in security breaches involving PII throughout the country has contributed to the loss of millions of records over the past few years. Security breaches involving PII are harmful to both organizations and individuals. Organizational damages may include a loss of public trust, legal liability, or remediation costs. Individual damages may include identity theft, embarrassment, or blackmail.

According to the United States Government Accountability Office, PII is any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

PII includes, but is not limited to:

- Name, such as full name, maiden name, mother‘s maiden name, or alias;
- Personal identification number, such as social security number, passport number, driver‘s license number, taxpayer identification number, or financial account or credit card number;
- Address information, such as street address or email address;
- Personal characteristics, including photographic image (especially of face or other identifying characteristic), fingerprints, handwriting, or other biometric data (e.g., retina scan, voice signature, facial geometry); and
- Information about an individual that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, weight, activities, geographical indicators, employment information, medical information, education information, financial information).

The Control Objectives for Information and Related Technology (COBIT) and National Institute of Standards and Technology (NIST) have established best practices for PII including collecting, classifying, inventorying, safeguarding and responding to data breaches.

COBIT 5 is a framework created by the Information Systems Audit and Control Association (ISACA) for Information Technology (IT) governance and management. Furthermore, COBIT 5:

- Provides a comprehensive framework that assists enterprises in achieving their objectives for the governance and management of enterprise IT.
- Helps enterprises create optimal value from IT by maintaining a balance between realizing benefits and optimizing risk levels and resource use.
- Enables IT to be governed and managed in a holistic manner for the entire enterprise, taking in the full end-to-end business and IT functional areas of responsibility, considering the IT-related interests of internal and external stakeholders.
- Is generic and useful for enterprises of all sizes, whether commercial, not-for-profit or in the public sector.

The Information Technology Laboratory (ITL) at NIST promotes the U.S. economy and public welfare by providing technical leadership for the nation‘s measurement and standards infrastructure. The Special Publication 800-series reports on ITL‘s research, guidance, and outreach efforts in computer security and its collaborative activities with industry, government, and academic organizations. NIST Special Publication 800-122 Guide to Protecting the Confidentiality of Personally Identifiable Information was used as criteria for this audit.

The City has adopted a Sensitive Data Policy that includes the handling, use, and safeguarding of

PII. This policy applies to all City employees, contractors, consultants, vendors, temporary employees, volunteers, and other workers at the City to include personnel affiliated with third parties doing business with the City. Under the Sensitive Data Policy, PII is classified as sensitive data and is the responsibility of each individual with access to sensitive data to safeguard this data.

Safeguards of PII are important to ensure the City is protecting PII from loss, theft, or misuse while simultaneously supporting the City's mission. The following are examples of safeguards:

- Administrative Safeguards - Training personnel on PII best practices;
- Physical Safeguards - Ensuring paper records and systems are secured and access is controlled; and
- Technical Safeguards - Encrypting system transmissions and emails, and requiring user access and login restrictions for systems.

The City must protect the PII of its citizens, employees, contractors, consultants, vendors, temporary employees, volunteers, and other workers at the City to include personnel affiliated with third parties doing business with the City.

For the purpose of safeguarding against and responding to the breach of PII the term "breach" is used to include the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to PII, whether physical or electronic. Failure to properly safeguard PII could lead to data breaches and unauthorized recipients may fraudulently use the information resulting in damage to victims.

FINDINGS

The following findings address areas that OIA believes could be improved by the implementation of the related recommendations.

1. DTI SHOULD MAINTAIN AN ACTIVE INVENTORY OF SYSTEMS AND DEVICES CONTAINING PII.

   The Department of Technology & Innovation (DTI) does not maintain an active inventory of systems and devices that contain PII. According to DTI management, the City does not track citywide PII and there is not a complete listing of citywide systems and devices containing PII. If an active inventory is not maintained, systems or devices containing PII might not be identified and properly classified or safeguarded.

   In an effort to determine if, the City maintains a comprehensive listing of systems, and

devices that contain PII, OIA:

- Requested DTI to provide a list of citywide systems and indicate which systems contain PII,
- Tested three systems significant to City operations that were not identified as having PII, and
- Identified 27,037 records containing high-risk PII in one of the three systems identified as not having PII.

DTI immediately began safeguarding the high-risk PII records as soon as OIA informed them of the issue.

If systems containing PII are not identified, data may be breached and result in the City incurring significant costs. For example, according to the 2018 Cost of Data Breach Study - Global Overview, performed by the Ponemon Institute LLC, the average cost per record breached is $148 per record. A breach of the 27,037 records would result in a cost of approximately $4 million to the City.

The Ponemon Institute is considered the pre-eminent research center dedicated to privacy, data protection and information security policy. Their annual consumer studies on privacy trust are widely quoted in the media and our research quantifying the cost of a data breach has become valuable to organizations seeking to understand the business impact of lost or stolen data.

COBIT 5 recommends that, "Management should create and maintain an inventory of information (systems and data) that includes a listing of owners, custodians and classifications. Include systems that are outsourced and those for which ownership should stay within the enterprise."

NIST recommends that organizations should:

- Identify all PII residing in their environment. An organization cannot properly protect PII it does not know about; and
- Regularly review their holdings of previously collected PII to determine whether the PII is still relevant and necessary for meeting the organization's business purpose and mission. If PII is no longer relevant and necessary, then it should be properly destroyed.

According to DTI management, the City does not track PII and there is not a complete citywide listing of systems and devices containing PII. In addition, DTI management stated that they were unaware of the 27,037 PII records identified by OIA because it is legacy information used for billing purposes, which has remained on the City system since fiscal year 2013.

RECOMMENDATION

DTI should review:

- Internal controls, develop processes, and assign responsibility to ensure that an active inventory of systems and devices containing PII is maintained.
- All citywide information systems to ensure that all PII is identified, classified, and safeguarded.
- Identified PII and determine if it is relevant and necessary to maintain.
- User access and ensure only those employees with a need to know should be authorized to access PII.

RESPONSE FROM DTI

"The Department of Technology and Innovation agrees with this finding and the recommendation."

ESTIMATED COMPLETION DATE

- ***"Review Internal controls, develop processes, and assign responsibility…: May 31, 2019***
- ***Review All citywide information systems to ensure…: April 15, 2019***
- ***Review Identified PII and determine…: As identified with initial determinations by April 15, 2019.***
- ***Review User access and ensure only those employees…: As identified with initial determinations by April 15, 2019."***

2. DTI SHOULD DEVELOP COMPREHENSIVE POLICIES AND PROCEDURES FOR CLASSIFYING AND SAFEGUARDING PII.

Overall, the City does not have comprehensive policies and procedures that would enable City departments to classify and safeguard PII including intake points, release/sharing points and storage. If controls are not in place to classify and safeguard PII, department personnel might not know the appropriate steps to take for specific data breach types, such as personal health information, governed by the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

OIA completed the following steps to determine what controls are in place at the department

level for classifying and safeguarding PII:

A. Toured and observed Department sites,
B. Gathered information via questionnaires, and
C. Reviewed current policies and procedures.

Since DTI does not maintain a complete inventory of citywide systems and devices containing PII (as identified in finding #1), OIA randomly selected 13 City departments to tour and observe in order to determine what controls are in place at the department level for classifying and safeguarding PII. After meeting with three departments and reviewing their processes for classifying and safeguarding PII, it was determined that none of them had established processes or specific policies and procedures for classifying and safeguarding PII, and additional systems containing PII were identified that were not included in the citywide listing of systems containing PII identified by DTI.

Since none of the three departments have established policies and procedures, OIA distributed a PII questionnaire to the 10 remaining departments, which determined that the City does not have a uniform approach for classifying and safeguarding PII.

The City has not developed comprehensive controls to classify and safeguard PII, and delegates responsibility to department directors for systems outside the DTI network. It is apparent that a comprehensive centralized approach should be taken to classify and safeguard PII.

The following sub-sections provide further details about the audit activities performed above (**A-C**).

A. <u>Toured and Observed</u>

During the tour and observation of the three departments, eight external cloud based systems and five internal systems were reviewed to determine what controls are in place for classifying and safeguarding PII.

The review of the eight external cloud based systems identified that none of the eight associated vendor contracts include clauses for classifying and safeguarding PII, and none of the three departments are regularly receiving and reviewing the Service and Organization Control Report (SOC) from the vendors. A SOC report is report provided by an external audit organization that evaluates the organization's information systems relevant to security, availability, processing integrity, confidentiality, or privacy.

COBIT 5 recommends that management, “Assess the status of external service providers’ internal controls and confirm that service providers comply with legal and regulatory requirements and contractual obligations.”

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) acknowledges that entities understand activities and controls associated with services received by outsourced service providers. According to the COSO Framework, principle 16, entities that use outsourced service providers for services such as third party warehousing, internet hosting, healthcare claims processing, retirement plan administration, or loan services need to understand the activities and controls associated with the services and how the outsourced service provider's internal control system affects the entity's system of internal control.

The review of the five internal systems identified that the departments could not provide information to verify if PII is classified and safeguarded. Furthermore, departments referred OIA to DTI for four of five systems. DTI responded to the questionnaire for two of the four systems, but did not respond for the other two. Based on the responses by DTI, it is unclear if PII is properly classified and safeguarded.

During the tour and observations an additional stand-alone system containing PII was identified that was not connected to the City network. This system has approximately 2,500 PII records.

According to 2018 Cost of Data Breach Study conducted by the Ponemon Institute LLC, the average cost of a lost or stolen PII record is $148 per record. A breach of the 2,500 records would result in a cost of approximately $370 thousand to the City.

COBIT 5 states that management should align the IT control environment with the overall IT policy environment, IT governance and IT process frameworks, and existing enterprise-level risk and control frameworks. Assess industry-specific good practices or requirements (e.g., industry-specific regulations) and integrate them where appropriate.

B. Gathered Information via Questionnaires

A questionnaire was used to identify and quantify information relating to the controls in place for intake, storage/disposal, and release/sharing of PII for the 10 remaining departments.

None of the departments have specific processes or policies and procedures for classifying and safeguarding PII. In addition, overall responses by the 10 departments indicate that the City does not have a uniform approach for classifying and safeguarding PII. **Appendix B** contains a summary of key points identified from the responses to the PII questionnaire by the 10 departments.

COBIT 5 states that management should:

- Create a set of policies to drive the IT control expectations on relevant key topics such as quality, security, confidentiality, internal controls, usage of IT assets, ethics and intellectual property rights.
- Ensure that the information communicated encompasses a clearly articulated mission, service objectives, security, internal controls, quality, code of ethics/conduct, policies and procedures, roles and responsibilities, etc. Communicate the information at the appropriate level of detail for the respective audiences within the enterprise.

The City's Sensitive Data Policy defines certain information as being sensitive, but does not provide full data classification guidance, nor does it include a privacy policy or media handling process.

When OIA initially requested PII policies and procedures from the 13 sampled departments:

- Seven departments stated that they either do not have departmental policies and procedures for classifying and safeguarding PII because they follow those established by DTI, or they do not have established PII policies and procedures, and
- Six did not respond.

The City's IT Protection Policy delegates the responsibility of protecting information technology assets under the physical control of departments to the department directors.

Many directors might not have the skill-set or staff to adequately protect information technology assets or to properly classify and safeguard PII, and will therefor rely on City IT policies for guidance. However, the current City Sensitive Data Policy does not provide the needed guidance to departments for adequately classifying and safeguarding PII.

C. Reviewed Policies and Procedures

The City Computer Security Incident Response Policy is not an incident response and data breach notification plan. It instead includes definitions, identifies members of the incident response team, and describes incidents and security breaches. The City does not have policies and procedures that fully address data breaches, or how to report a data breach within the City and externally if required by contracts, laws, or regulations. Without policies and procedures, an actual data breach might be unidentified or ignored and result in higher compliance costs.

The following guidelines provide control suggestions for data breaches.

- NIST – Organizations should consider developing privacy policies and associated

procedures for PII incident response and data breach notification.

- COBIT 5 – Management should apply data classification and acceptable use and security policies and procedures to protect information assets under the control of the business. Management should identify and implement processes, tools and techniques to reasonably verify compliance.

The following regulations provide control requirements for data breaches, and require different actions for data breaches.

- The New Mexico Data Breach Notification Act – Requires service providers to implement and maintain reasonable security procedures and practices appropriate to the nature of the personal identifying information and to protect it from unauthorized access, destruction, use, modification or disclosure.
- HIPAA § 164.414 Final Rule – We emphasize the importance of ensuring that all workforce members are appropriately trained and knowledgeable about what constitutes a breach and on the policies and procedures for reporting, analyzing, and documenting a possible breach of unsecured protected health information.
- Family Educational Rights and Privacy Act of 1974 FERPA § 99.35 (3) (C) (v) – Establish policies and procedures, consistent with the Act and other Federal and State confidentiality and privacy provisions, to protect personally identifiable information from education records from further disclosure (except back to the disclosing entity) and unauthorized use, including limiting use of personally identifiable information from education records to only authorized representatives with legitimate interests in the audit or evaluation of a Federal or State supported education program or for compliance or enforcement of Federal legal requirements related to these programs.
- Payment Card Industry Data Security Standard (PCI DSS) 12.10 – Implement an incident response plan. Be prepared to respond immediately to a system breach.
- PCI DSS 12.10.1 - Create the incident response plan to be implemented in the event of system breach.

According to DTI management, data breach, including properly classifying and safeguarding PII, was previously not a huge concern for a local government that had transparency laws requiring it to release requested data.

RECOMMENDATIONS

DTI should:

- Develop comprehensive policies and procedures for classifying and safeguarding PII. The policies and procedures should include:
  - City departments' guidelines for classifying and safeguarding the

intake, storage/disposal, and release/sharing of PII.
  - Guidelines for handling a data breach that specifically address which regulations apply and who to notify depending on the type of data involved. **Appendix C** includes a PII Regulations Matrix that lists various regulations, the type of entity that may be affected by the regulation, what is determined to be PII, and what should be done if the event of a data breach.
- Review its current practices including IT functions maintained by City departments outside of DTI's main authority and develop citywide policies and procedures that address data breaches.

RESPONSE FROM DTI

"The Department of Technology and Innovation agrees with this finding and the recommendations."

ESTIMATED COMPLETION DATES

- ***"Develop comprehensive policies and procedures for classifying and safeguarding PII: July 31, 2019***
- ***Review its current practices including IT functions…: March 31, 2019"***

3. DTI SHOULD ENSURE THAT EMPLOYEES WITH ACCESS TO PII ARE TRAINED AND AWARE OF THEIR RESPONSIBILITY TO SAFEGUARD PII.

Individuals with access to the City's computer environment are not always trained or aware of their responsibility to safeguard PII. The table below summarizes the results of 24 individuals interviewed and tested regarding their training and awareness of their responsibility to safeguard PII. For example, of the 24 individuals tested 16 (67-percent) had not received training for safeguarding PII.

Summary of Questionnaire Results for Twenty-Four Individuals with Access to the City's Computer Environment

Questions for City employees with access to computer environment	Yes	No	Don't know/Not sure/Not aware	Inform Supervisor and/or DTI	Other

Questions for City employees with access to computer environment	Yes	No	Don't know/Not sure/Not aware	Inform Supervisor and/or DTI	Other
Are you familiar with Personal Identifiable Information (PII)?	22	2			
Do you use or maintain PII?	19	5			
Are you aware of any systems, databases, etc. that your department uses that contain PII?	15	9			
Does your department share PII with other departments or entities?	6	5	13		
Does your department have established specific policies and procedures for classifying and safeguarding PII?		19	5		
Are you aware of City policies for safeguarding PII?	9	14	1		
What would you do if a data breach occurred? (1)			1	21	2
Have you received training for safeguarding PII? (2)	8	16			
Does your computer hard and/or shared network drive contain PII accessible to multiple individuals? (3)	5	17			2

Source: Responses to questionnaire

(1) – Other Responses: Contact federal funding source; and research and try to correct
(2) – Verified using the training Enrollment/Completion report from DTI
(3) – Two individuals did not bring their computers to the interview

While performing test work, OIA identified 1,805 PII records that are accessible to multiple users on computers of five employees (21-percent). According to 2018 Cost of Data Breach Study conducted by the Ponemon Institute LLC, the average cost of a lost or stolen PII record is $148 per record. A breach of these records could result in the City incurring a cost of approximately $267 thousand.

According to NIST:

- PII should be protected through a combination of measures, including operational safeguards, privacy specific safeguards, and security controls;
- An organization that is subject to any obligations to protect PII should consider such

obligations when determining the PII confidentiality impact level. Many organizations are subject to laws, regulations, or other mandates governing the obligation to protect personal information, such as the Privacy Act of 1974, and HIPAA;

- Decisions regarding the applicability of a particular law, regulation, or other mandate should be made in consultation with an organization‘s legal counsel and privacy officer because relevant laws, regulations, and other mandates are often complex and change over time; and
- Organizations should reduce the possibility that PII will be accessed, used, or disclosed inappropriately by requiring that all individuals receive appropriate training before being granted access to systems containing PII.

DTI has implemented a mandatory annual security refresher course and created a PII awareness section on the City's SharePoint site. However, individuals with access to the City's computer environment are not always aware of City policies for safeguarding PII. Those who stated they are aware of safeguarding PII policies could not specifically name them, or discuss them in general. As a result, City employees are not always trained on safeguarding PII.

RECOMMENDATION

After DTI creates comprehensive PII processes, policies, and procedures to classify and safeguard PII, DTI should:

- Train City department staff on classifying and safeguarding PII.
- Communicate regularly with City departments to ensure that all individuals with access to the computer environment are trained on and aware of the City’s policies and procedures on PII and their responsibility for safeguarding PII.

RESPONSE FROM DTI

“The Department of Technology and Innovation agrees with this finding and the recommendations.”

ESTIMATED COMPLETION DATE

- ***“Train City department staff on classifying and safeguarding PII.: October 31, 2019***
- ***Communicate regularly with City departments…: Beginning September 1, 2019, with ongoing frequency to be included in policies and procedures to be developed.”***

CONCLUSION

Current citywide processes, policies and procedures are not adequate to ensure classifying and safeguarding of PII at the department level, and delegate certain authority to the department directors.

DTI does not maintain an active inventory of systems and devices that contain PII. The City also does not have comprehensive policies and procedures for classifying and safeguarding PII. In addition, individuals with access to the City's computer environment are not always trained on or aware of their responsibility to safeguard PII.

DTI can effectively manage PII security on City systems by:

- Maintaining an active inventory of systems and devices containing PII,
- Ensuring policies and procedures and underlying controls for classifying and safeguarding PII at the department level are established, and
- Ensuring that employees with access to PII are trained on and aware of their responsibility to safeguard PII.

We greatly appreciate the assistance, involvement, and cooperation of DTI and department management. Their time, assistance, involvement, and cooperation are greatly appreciated.

PII Security on City Systems
Citywide 18-103
February 27, 2019

PREPARED:

_____
Alan R. Gutowski, Senior Information Systems Auditor
Office of Internal Audit

REVIEWED:

_____
Lawrence L. Davis, Internal Audit Manager
Office of Internal Audit

APPROVED:

_____
Jim Thompson, City Auditor
Office of Internal Audit

APPROVED FOR PUBLICATION**:**

_____
Edmund E. Perea, Chairperson, Accountability in
Government Oversight Committee

APPENDIX A

OBJECTIVES

The audit objectives were to determine:

1. Does the City of Albuquerque (City) maintain an active listing of systems and devices that contain personal identifiable information (PII)?
2. Does the City have controls in place to classify and safeguard PII including intake points, release/data sharing points and storage?
3. Are individuals with access to the City's computer environment trained on and aware of their responsibility to safeguard PII?

SCOPE AND LIMITATIONS

Our audit did not include an examination of all functions and activities related to PII on citywide systems. Our scope was limited to the objectives above. This report and its conclusions are based on information taken from a sample of departments, systems, and users and do not represent an examination of all related departments, systems, and users. The audit report is based on our examination of functions and activities through the completion of fieldwork on January 23, 2019, and does not reflect events after that date.

Management of the Department of Technology & Innovation as well as departmental management throughout the City are responsible for classifying and safeguarding PII, establishing and maintaining effective internal controls, complying with City Information Technology (IT) policies and standards, and applicable laws, regulations, standards, guidelines, contracts and best practices for classifying and safeguarding PII.

In performance audits, a deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct (1) impairments of effectiveness or efficiency of operations, (2) misstatements in financial or performance information, or (3) noncompliance with applicable laws, regulations, standards, guidelines, and/or best practices for safeguarding PII. A deficiency in design exists when (a) a control necessary to meet the control objective is missing or (b) and existing control is not properly designed so that, even if the control operates as designed, the control objective is not met. In the performance audit requirements, the term significant is comparable to the term material as used in the context of financial statement engagements. A deficiency in operation exists when a properly designed control does not operate as designed, or when the person performing the control does not possess

the necessary authority or qualifications to perform the control effectively.

Our consideration of internal control was for the limited purpose described in our audit objectives and was not designed to identify all deficiencies in internal control. Therefore, unidentified deficiencies may exist. Accordingly, we do not express an opinion on the effectiveness of the City's internal control.

As part of the performance audit, we tested the City's compliance with applicable laws, regulations, standards, guidelines, contracts and/or best practices for classifying and safeguarding PII. Noncompliance with these requirements could directly and significantly affect the objectives of our audit. However, opining on compliance with all provisions was not an objective of our performance audit and accordingly, we do not express an opinion.

We conducted this performance audit in accordance with generally accepted government auditing standards for performance audits, as prescribed in *Government Auditing Standards*, revision 2011, issued by the Controller General of the United States. 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.

METHODOLOGY

Methodologies used to accomplish the audit objectives include but are not limited to the following,

- Inquired with City departments and DTI to identify all City systems including those containing PII,
- Selected a random statistical sample of City departments,
- Met with departments and performed walk-throughs, to determine controls in place to classifying and safeguard PII,
- Inquired with departments to determine how PII is classified and safeguarded,
- Surveyed a random statistical sample of departmental directors regarding intake, storage/disposal, and release/sharing of PII,
- Selected a judgmental sample of City systems not identified as containing PII,
- Queried sampled systems for PII,
- Reviewed City IT policies and procedures pertaining to PII,
- Reviewed applicable laws, regulations, standards, guidelines, contracts and/or best practices for classifying and safeguarding PII,
- Selected a random statistical sample of active users with access to the City's computer

environment,

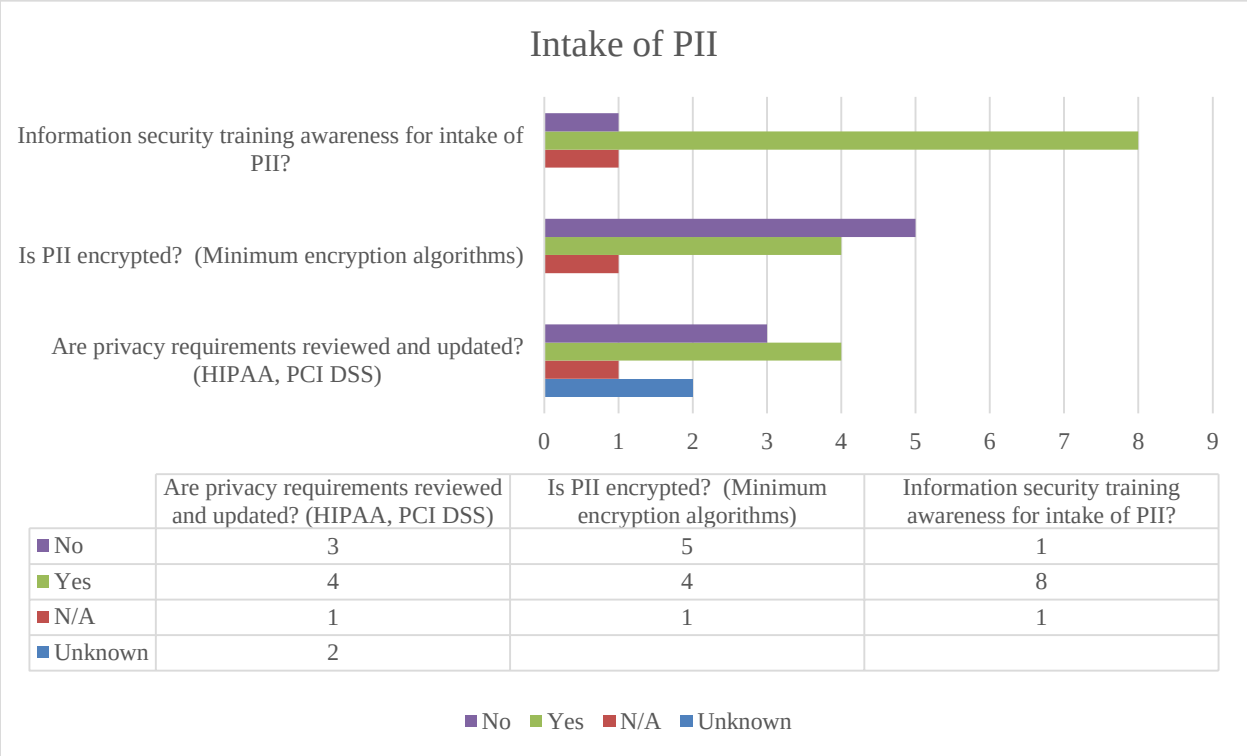
- Surveyed sampled users to determine if they are trained on and aware of their responsibility to safeguard PII, and
- Inquired with DTI management to determine how they ensure users are trained on and aware of their responsibility to safeguard PII.

APPENDIX B

Key Points Identified from Questionnaire Responses (10)

Intake of PII

Departments are receiving awareness training for intake of PII, but PII is not always encrypted and privacy requirements are not always reviewed and updated. The graph and table below summarize key points from questionnaire responses regarding the intake of PII.

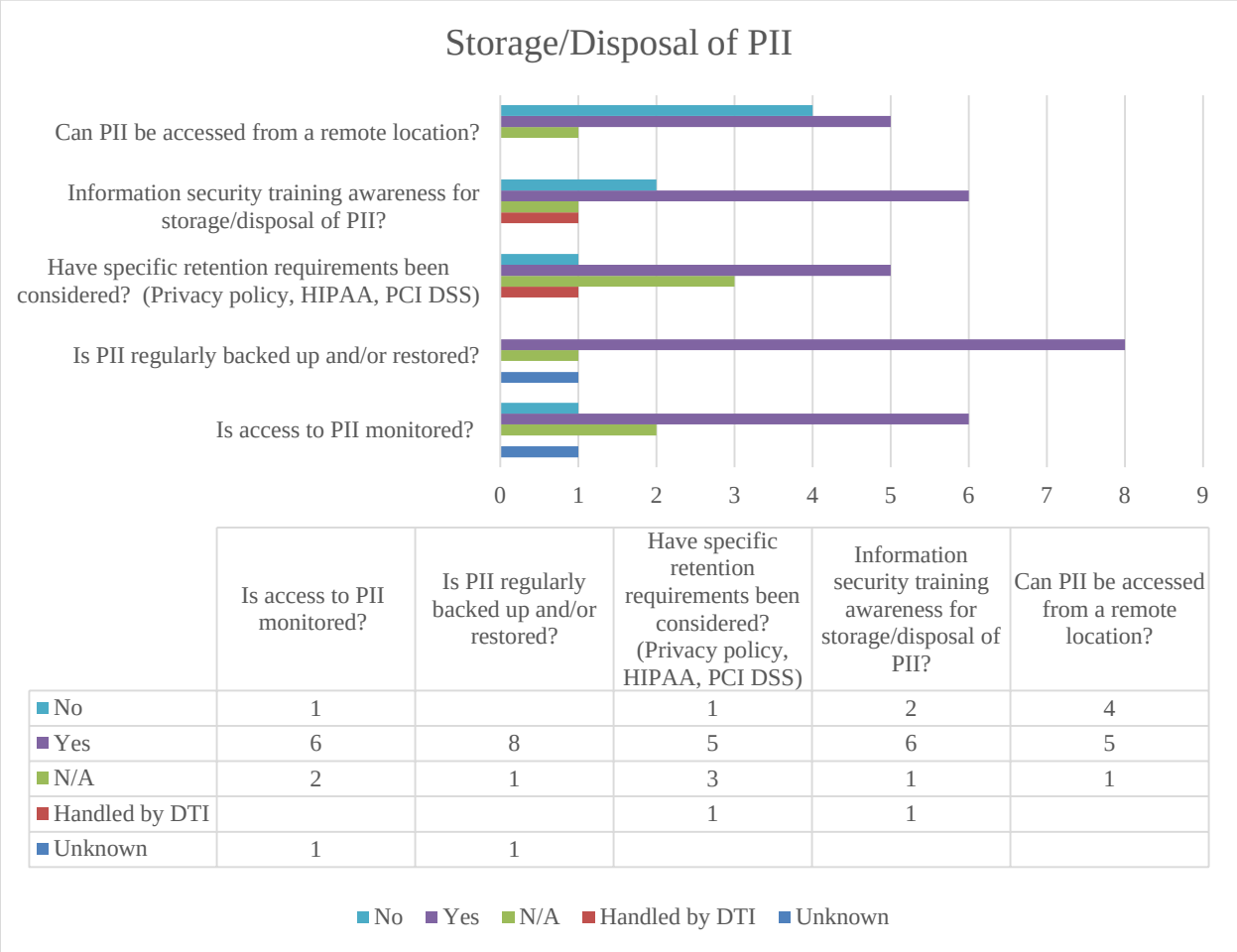


	Are privacy requirements reviewed and updated? (HIPAA, PCI DSS)	Is PII encrypted? (Minimum encryption algorithms)	Information security training awareness for intake of PII?
No	3	5	1
Yes	4	4	8
N/A	1	1	1
Unknown	2		

Source: City Departments

Storage/Disposal of PII

Departments are receiving awareness training for storage/disposal of PII. The majority of departments regularly back- up, monitor access to, and consider retention requirements of PII. However, PII can be accessed from remote locations exposing PII to greater risk of breach. The graph and table below summarize key points from questionnaire responses regarding the storage/disposal of PII.

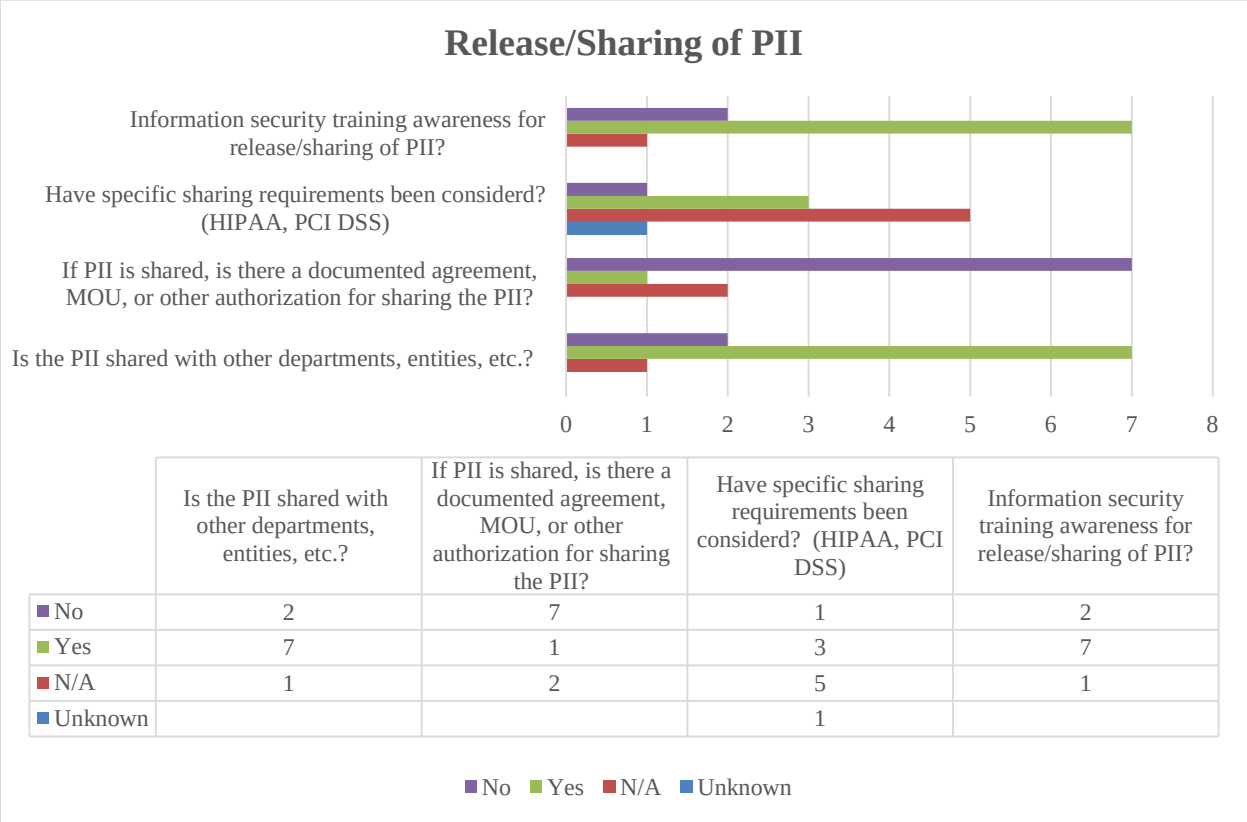


	Is access to PII monitored?	Is PII regularly backed up and/or restored?	Have specific retention requirements been considered? (Privacy policy, HIPAA, PCI DSS)	Information security training awareness for storage/disposal of PII?	Can PII be accessed from a remote location?
No	1		1	2	4
Yes	6	8	5	6	5
N/A	2	1	3	1	1
Handled by DTI			1	1	
Unknown	1	1			

Source: City Departments

Release/Sharing of PII

Departments are receiving awareness training for release/sharing of PII. PII is shared with other departments, entities, etc., but protective sharing requirements are not always considered. Furthermore, the sharing of PII with others is not always documented in a formal agreement. The graph and table below summarize key points from questionnaire responses regarding the release/sharing of PII.



	Is the PII shared with other departments, entities, etc.?	If PII is shared, is there a documented agreement, MOU, or other authorization for sharing the PII?	Have specific sharing requirements been considerd? (HIPAA, PCI DSS)	Information security training awareness for release/sharing of PII?
No	2	7	1	2
Yes	7	1	3	7
N/A	1	2	5	1
Unknown			1	

Source: City Departments

Appendix C

PII Regulations Matrix

Regulation	Responsible Entity	Applicable PII	Process for Data Breach
Health Insurance Portability and Accountability Act of 1996 (HIPAA)	**§ 160.103 Definitions.** **(**3) Business associate includes: (i) A Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to protected health information to a covered entity and that requires access on a routine basis to such protected health information. (ii) A person that offers a personal health record to one or more individuals on behalf of a covered entity. (iii) A subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate.	**§ 160.103 Definitions.** Protected health information means individually identifiable health information: (1) Except as provided in paragraph (2) of this definition, that is: (i) Transmitted by electronic media; (ii) Maintained in electronic media; or (iii) Transmitted or maintained in any other form or medium. (2) Protected health information excludes individually identifiable health information: (i) In education records covered by the Family Educational	**§ 164.404 Notification to individuals.** (a) Standard — (1) General rule. A covered entity shall, following the discovery of a breach of unsecured protected health information, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of such breach. Except as provided in § 164.412, a covered entity shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 calendar days after discovery of a breach. **§ 164.408 Notification to the Secretary.** (a) Standard. A covered entity shall, following the discovery of a breach of unsecured protected health information as provided in § 164.404(a) (2), notify the Secretary. **§ 164.412 Law enforcement delay.** If a law enforcement official states to a covered entity or business associate that a notification, notice, or posting required under this subpart would impede a criminal investigation or cause damage to national security, a covered entity or business associate shall: (a) If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting for the time period specified by the official; or b) If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described in paragraph (a) of this section is submitted during that time.

Regulation	Responsible Entity	Applicable PII	Process for Data Breach
		Rights and Privacy Act, as amended, 20 U.S.C. 1232g; (ii) In records described at 20 U.S.C. 1232g(a)(4)(B)(iv); (iii) In employment records held by a covered entity in its role as employer; and (iv) Regarding a person who has been deceased for more than 50 years.	

Regulation	Responsible Entity	Applicable PII	Process for Data Breach
Family Educational Rights and Privacy Act (FERPA)	(Authority: 20 U.S.C. 1232g(b)(1) and (b)(2)) "Early childhood education program" means – (a) A Head Start program or an Early Head Start program carried out under the Head Start Act (42 U.S.C. 9831 et seq.), including a migrant or seasonal Head Start program, an Indian Head Start program, or a Head Start program or an Early Head Start program that also receives State funding; (b) A State licensed or regulated child care program; or (c) A program that – (1) Serves children from birth through age six that addresses the children's cognitive (including language, early literacy, and early mathematics), social, emotional, and physical	(Authority: 20 U.S.C. 1232g(b)(4)(A)) "Personally Identifiable Information" The term includes, but is not limited to-- (a) The student's name; (b) The name of the student's parent or other family members; (c) The address of the student or student's family; (d) A personal identifier, such as the student's social security number, student number, or biometric record; (e) Other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name; (f) Other information that, alone or in combination, is linked or linkable to a specific	(Authority: 20 U.S.C. 1232g(b)(4)(B), (f), and (g)) (c) If the Office finds that a third party, outside the educational agency or institution, violates § 99.31(a)(6)(iii)(B), then the educational agency or institution from which the personally identifiable information originated may not allow the third party found to be responsible for the violation of §99.31(a)(6)(iii)(B) access to personally identifiable information from education records for at least five years. (d) If the Office finds that a State or local educational authority, a Federal agency headed by an official listed in § 99.31(a)(3), or an authorized representative of a State or local educational authority or a Federal agency headed by an official listed in § 99.31(a)(3), improperly rediscloses personally identifiable information from education records, then the educational agency or institution from which the personally identifiable information originated may not allow the third party found to be responsible for the improper redisclosure access to personally identifiable information from education records for at least five years. (e) If the Office finds that a third party, outside the educational agency or institution, improperly rediscloses personally identifiable information from education records in violation of § 99.33 or fails to provide the notification required under § 99.33(b)(2), then the educational agency or institution from which the personally identifiable information originated may not allow the third party found to be responsible for the violation access to personally identifiable information from education records for at least five years.

Regulation	Responsible Entity	Applicable PII	Process for Data Breach
	development; and (2) Is – (i) A State prekindergarten program; (ii) A program authorized under section 619 or part C of the Individuals with Disabilities Education Act; or (iii) A program operated by a local educational agency. "Education program" means any program that is principally engaged in the provision of education, including, but not limited to, early childhood education, elementary and secondary education, postsecondary education, special education, job training, career and technical education, and adult education, and any program that is administered by an educational agency or institution.	student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; or (g) Information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education record relates.	

Regulation	Responsible Entity	Applicable PII	Process for Data Breach
Payment Card Industry Data Security Standard (PCI DSS	PCI DSS applies to all entities involved in payment card processing—including merchants, processors, acquirers, issuers, and service providers. PCI DSS also applies to all other entities that store, process or transmit cardholder data (CHD) and/or sensitive authentication data (SAD).	Cardholder Data includes: • Primary Account Number (PAN) • Cardholder Name • Expiration Date • Service Code Sensitive Authentication Data includes: • Full track data (magnetic-stripe data or equivalent on a chip) • CAV2/CVC2/CVV2/CID • PINs/PIN blocks	**12.10** Implement an incident response plan. Be prepared to respond immediately to a system breach. **12.10.1** Create the incident response plan to be implemented in the event of system breach. Ensure the plan addresses the following, at a minimum: • Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum. • Specific incident response procedures. • Business recovery and continuity procedures. • Data backup processes. • Analysis of legal requirements for reporting compromises. • Coverage and responses of all critical system components. • Reference or inclusion of incident response procedures from the payment brands.

Regulation	Responsible Entity	Applicable PII	Process for Data Breach
New Mexico Data Breach Notification Act	SECTION 8. EXEMPTIONS.-- The provisions of the Data Breach Notification Act shall not apply to a person subject to the federal Gramm-Leach-Bliley Act or the federal Health Insurance Portability and Accountability Act of 1996.	C. "personal identifying information": (1) means an individual's first name or first initial and last name in combination with one or more of the following data elements that relate to the individual, when the data elements are not protected through encryption or redaction or otherwise rendered unreadable or unusable: (a) social security number; (b) driver's license number; (c) government-issued identification number; (d) account number, credit card number or debit card number in combination with any required security code, access code or	SECTION 6. NOTIFICATION OF SECURITY BREACH.-- A. Except as provided in Subsection C of this section, a person that owns or licenses elements that include personal identifying information of a New Mexico resident shall provide notification to each New Mexico resident whose personal identifying information is reasonably believed to have been subject to a security breach. Notification shall be made in the most expedient time possible, but not later than forty-five calendar days following discovery of the security breach, except as provided in Section 9 of the Data Breach Notification Act. B. Notwithstanding Subsection A of this section, notification to affected New Mexico residents is not required if, after an appropriate investigation, the person determines that the security breach does not give rise to a significant risk of identity theft or fraud. C. Any person that is licensed to maintain or possess computerized data containing personal identifying information of a New Mexico resident that the person does not own or license shall notify the owner or licensee of the information of any security breach in the most expedient time possible, but not later than forty-five calendar days following discovery of the breach, except as provided in Section 9 of the Data Breach Notification Act; provided that notification to the owner or licensee of the information is not required if, after an appropriate investigation, the person determines that the security breach does not give rise to a significant risk of identity theft or fraud.

Regulation	Responsible Entity	Applicable PII	Process for Data Breach
		password that would permit access to a person's financial account; or (e) biometric data; and (2) does not mean information that is lawfully obtained from publicly available sources or from federal, state or local government records lawfully made available to the general public	D. A person required to provide notification of a security breach pursuant to Subsection A of this section shall provide that notification by: (1) United States mail; (2) electronic notification, if the person required to make the notification primarily communicates with the New Mexico resident by electronic means or if the notice provided is consistent with the requirements of 15 U.S.C. (3) a substitute notification, if the person demonstrates that: (a) the cost of providing notification would exceed one hundred thousand dollars ($100,000); (b) the number of residents to be notified exceeds fifty thousand; or (c) the person does not have on record a physical address or sufficient contact information for the residents that the person or business is required to notify. E. Substitute notification pursuant to Paragraph (3) of Subsection D of this section shall consist of: (1) sending electronic notification to the email address of those residents for whom the person has a valid email address; (2) posting notification of the security breach in a conspicuous location on the website of the person required to provide notification if the person maintains a website; and (3) sending written notification to the office of the attorney general and major media outlets in New Mexico. F. A person that maintains its own notice

Regulation	Responsible Entity	Applicable PII	Process for Data Breach
			procedures as part of an information security policy for the treatment of personal identifying information, and whose procedures are otherwise consistent with the timing requirements of this section, is deemed to be in compliance with the notice requirements of this section if the person notifies affected consumers in accordance with its policies in the event of a security breach.

Source: Various regulations identified in table