City of Albuquerque

Office of Internal Audit

FOLLOW-UP OF THE
PERSONABLE IDENTIFIABLE INFORMATION (PII)
SECURITY ON CITY SYSTEMS – CITYWIDE AUDIT
Report #20-18-103F
March 11, 2021

INTRODUCTION

The Office of Internal Audit (OIA) issued Audit No. 18-103, Personable Identifiable Information (PII) Security on City Systems – Citywide on February 27, 2019. OIA has completed a follow-up to determine the corrective actions that the Department of Technology & Innovations (DTI) has taken in response to the report. The report contains three recommendations, two of which have been implemented and are now closed, and one that remains in progress.

BACKGROUND

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 October 2, 2018 through 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 of the original audit report.

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. DTI is responsible for monitoring the security of the City's PII.

OBJECTIVE

The objective of this follow-up was to determine whether DTI has taken the corrective actions recommended in OIA's February 27, 2019 audit report regarding PII Security on City Systems. Consistent with Government Auditing Standards, Section 9.08, promulgated by the U.S. Government Accountability Office, the purpose of audit reports include facilitating a follow-up to determine whether appropriate corrective actions have been taken. This field follow-up is a non-audit service. Government Auditing Standards do not cover non-audit services, which are defined as professional services other than audits or attestation engagements. Therefore, DTI is responsible for the substantive outcomes of the work performed during this follow-up and is responsible to be in a position, in fact and appearance, to make an informed judgment on the results of the non-audit service. OIA limited our scope to actions taken to address our audit recommendation from the final audit report dated February 27, 2019 through the submission of actions on February 22, 2021.

METHODOLOGY

To achieve the objective, OIA:

- Obtained documentary evidence from DTI.
- Interviewed DTI to understand and verify the status and nature of the corrective actions taken.
- Verified the status of the recommendations that DTI had reported as implemented.

RESULTS

Of the three recommendations addressed in the original audit report, two have been closed, and one remains in progress. OIA will follow up on the status of the remaining open recommendation in six months.

See ATTACHMENT 1

SUBMITTED:

DocuSigned by:
Connie Barros-Montoya
DCF283F3AC33444...

Connie Barros-Montoya, Principal Auditor
Office of Internal Audit

REVIEWED :

DocuSigned by:
Sarah Faford-Johnson
15C18D8E99C84C1...

Sarah L. Faford-Johnson, Contract Auditor
Office of Internal Audit

APPROVED:

DocuSigned by:
Nicole Kelley
07E2FA5E2FAD4AC...

Nicole Kelley, Acting City Auditor
Office of Internal Audit

APPROVED FOR PUBLICATION:

DocuSigned by:
Edmund E. Perea, Esq.
645A1FA5A6314C3...

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

ATTACHMENT 1

Recommendation	Responsible Agency	Department Response	OIA Conclusion	20-18-103F OIA Use Only Status
Recommendation 1: The Department of Technology & Innovation (DTI) should review: - Internal controls, develop processes, and assign responsibility to ensure that an active inventory of systems and devices containing PII are 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.	Department Technology and Innovation	- DTI and Information Security Guidance Group (ISGG) has reviewed the PII systems and they are being inventoried in our asset management system. - DTI Security Group started meeting in FY20 with ISGG on the 3rd Thursday of the month to review internal controls and PII inventory, with the Infrastructure Manager. - Infrastructure Manager shall notify DTI Security Group which oversees the database and informs DTI of PII systems are setup and safeguarded. - DTI Security Group shall ensure the inventory is updated accordingly. - DTI Security Group shall review monthly with ISGG and Department Liaisons to ensure authorized PII access.	In March 2020, DTI Security Group began to meet monthly to review PII inventory with the Infrastructure Manager. During the meetings the Infrastructure Manager will notify DTI Security Group of any changes in PII systems and DTI Security Group will then be responsible for ensuring the PII inventory is updated accordingly. For non-DTI servers, DTI Security Group shall review monthly with ISGG and Department Liaisons to ensure PII's inventory. DTI also inventoried the PII systems in the City's asset management system and classified PII has been identified and encrypted. DTI reviewed user access to ensure only those employees with a need to know should be authorized to access PII.	☐ Open ☒ Closed ☐ Contested

ATTACHMENT 1

Recommendation	Responsible Agency	Department Response	OIA Conclusion	20-18-103F OIA Use Only Status
Recommendation 2: 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. - 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.	Department Technology and Innovation	DTI has a PII policy for the City of Albuquerque dated 1/13/2021 that was reviewed in conjunction with the Information Security Guidance Group (ISGG).	In January 2021 DTI developed comprehensive policies and procedures that classify the safeguard. However, the policy has not been officially approved by DTI director and therefore has not been communicated to city employees. The policy specifically, directs the intake, storage, disposal, releasing, and sharing of PII. Guidelines state that instances of unauthorized disclosure or access of PII, employees are to report the event immediately to their supervisor and report it to the help desk via email: ISDHelpdest@cabq.gov. According to DTI management, the policies and procedures are estimated to be approved and communicated to city employees before the end of the third quarter of fiscal year 2021.	☒ Open ☐ Closed ☐ Contested

ATTACHMENT 1

Recommendation	Responsible Agency	Department Response	OIA Conclusion	20-18-103F OIA Use Only Status
Recommendation 3: 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.	Department Technology and Innovation	DTI will begin PII Awareness Training in January 2021 starting with the DTI . DTI Personal Identifiable Information (PII) Awareness Curriculum: • The definition of PII • Applicable privacy laws, regulations, and policies • Restrictions on data collection, storage, and use of PII • Roles and responsibilities for using and protecting PII • Appropriate disposal of PII	DTI begun PII Awareness Training in January 2021, starting with the DTI Department. The web-based training will be deployed to subsequent departments throughout the City each month.	☐ Open ☒ Closed ☐ Contested