Auditing a Government's Protection of Personally Identifiable Information (PII)

Corrie Stokes
Acting City Auditor
Austin, Texas

December 2014

Auditing Protection of PII

What is Personally Identifiable Information (PII)?

Any data that can be used to identify someone or can be linked to a specific person. Examples include:

- Social security numbers
- Personal email addresses
- Fingerprints
- IP addresses
- Driver's license numbers
- Bank account information
- Medical information

3

Auditing Protection of PII

Why audit PII?

Unauthorized disclosure of PII can result in:

- Financial or medical information being compromised
- Identity theft
- Blackmail
- Violations of state or federal law
- Significant financial costs for the disclosing entity

4

Auditing Protection of PII

Our Objective

Evaluate process for protecting PII collected and/or stored by the City

Our Scope

Policies and procedures in FY13 for:

- SSNs
- Dates of birth
- Personal medical information
- Personal financial information

5

Auditing Protection of PII

Initial Audit Approach

Identify potential high-risk departments in terms of having and handling PII

Methodologies

- Survey all City departments
- Interview employees involved in the protection of PII
- Review related policies and training
- Research policies for protecting PII in other entities

Criteria

NIST's Guide to Protecting the Confidentiality of PII

6

Auditing Protection of PII

Overall Finding

The City does not have an effective process to ensure that PII is protected, which increases the risk that citizens, employees, or the City could face serious harm.

Survey Results

Most departments reported collecting PII from employees and/or citizens. For those departments:

- 52% did not have written policies/procedures
- 45% had employees who did not receive training
- 38% did not have someone responsible for PII

7

Auditing Protection of PII

Comparison to Best Practices from NIST

NIST Recommendations	City of Austin Audit Results
Identify PII	No method to identify PII
Categorize PII	No method to categorize PII
Policies and Procedures	Over half of departments reported not having policies and procedures related to the protection of PII
Training	Nearly half of departments reported their employees do not receive training related to the protection of PII
Incident Response Plan	No written plan to respond to the loss/misuse of PII

8

Auditing Protection of PII

Should my entity audit PII?

- Does your entity have data that can be used to identify someone?
- Does your entity have an inventory of that data?
- Is protection of that data covered in your entity's records management approach?
- Have you had prior findings related to safeguarding of hard-copy or electronic information?

Questions?

Audit Report on Protection of Personally Identifiable Information (PII) available at:
http://austintexas.gov/sites/default/files/files/Auditor/au13019.pdf

Contact Information:
Corrie Stokes
Office of the City Auditor
Austin, Texas
corrie.stokes@austintexas.gov
(512)974-2805