CITY OF WINSTON-SALEM CONTROLS OVER PERSONAL IDENTIFYING INFORMATION – GRANTEE AND DEBTOR DATA REVIEW

Submitted by:
Budget and Performance Management
Internal Audit Division
May 2022

Overview of Data Privacy

The City of Winston-Salem (City) maintains a vast amount of personal identifying information (PII) across a number of departments and operating areas. The data is often associated with activities related to grants, loans, vendors, contractors, permitting, employees, and customers. The departments with a significant amount of private data include Financial Management Services (Treasury, Risk Management, Purchasing, Accounting Services, Accounts Payable (AP), and Revenue), Human Resources, Community Development (CD), Business Inclusion and Advancement (BIA), and Police.

A City Council Resolution dated October 27, 2008 authorized the creation and implementation of an Identity Theft Prevention Program in conjunction with the Fair and Accurate Credit Act of 2003 (Red Flag Regulations). Some departments have procedures promoting the protection of PII but there are no known procedures concentrating specifically on data privacy or that apply across the City. The Information Systems Department (IS) has procedures in place for protecting the City network and databases.

Data Privacy Projects

The large amount of PII maintained by the City is complicated by the many different types of City activities. Each activity has unique data requirements and separate data repositories or databases. Moreover, each repository or database is subject to different management and controls. To make these projects more manageable, categories of PII have been broken-down into separate data groups of: 1) customer data, 2) vendor and contractor data, 3) permit data, 4) grantee and debtor data, 5) risk management data, 6) employee data, and 7) crime and victim data. Each of these data groups have had their own separate review performed. The primary focus of the data privacy review is being narrowed to sensitive PII. Sensitive PII is initially defined as driver's license (DL), social security number (SSN), tax identification number (TIN), passport or foreign ID, bank account information, bank card information, PIN, user ID and password, and latent prints (includes fingerprints); moreover, the following PII can also be considered sensitive (medical data, date of birth (DOB), or the last four digits of the SSN) when any of these are paired with another identifier. Sensitive PII should be subject to a higher degree of protection.

CD collects sensitive grantee and debtor PII from citizens. The Department of Transportation (DOT), Budget Division, and City Manager's Office (CMO) collect sensitive grantee PII from citizens. BIA and the Revenue Division collect sensitive debtor PII from citizens. This sensitive PII data can be collected in person and electronically. The performance of everyday activities may require the aforementioned departments and divisions to transmit PII and the data may be retained by application service providers. These departments and divisions have common process requirements, shared system applications, their own hardcopy files, and their own set of PII.

Scope of Review Procedures Performed

Interviews with each of the prior mentioned departments and divisions' staff were performed during March-April 2022. The information obtained from interviews was used to create a comprehensive inventory of sensitive PII by repository and to identify existing physical, electronic, and procedural controls

for the effective prevention of unauthorized access to sensitive PII. Representations obtained from these aforementioned departments and divisions were then evaluated for significant vulnerabilities.

The following charts outline the Sensitive PII Repositories found:

Controls Over PII - Grantee and Debtor Data		Sensitive PII							
Sensitive PII Repository (Location)	**Type of Information/Data**	**TIN**	**SSN**	**DOB**	**Last 4 of SSN**	**DL / State ID**	**Bank Account**	**Bank Card**	**Medical Data**
Grantee Data									
Partner connect	**DOT** - DBE-IS forms submitted for grant reimbursments.	X							
Enterprise Business System (EBS) portal	**DOT** - Payment information such as invoices and support documentation including proof of payment for grant reimbursements.	X					X		
Hard Drive	**CMO** - Scanned Request for Check support.	X							
Hardcopy in unsecured mailbox	**DOT** - 5310 or 5307 grant hardcopy printouts for reimbursement in the administrative secretary's inbox. Hardcopy provisional paperwork, includes subrecipient reimbursement supporting documents, in the Finance Manager and DOT Director's mailboxes.	X	X				X		
Hardcopy in unsecured area	**CMO** - Grant materials in unsecured office area or unsecured file cabinets.	X							

Controls Over PII - Grantee and Debtor Data		Sensitive PII							
Sensitive PII Repository (Location)	Type of Information/Data	TIN	SSN	DOB	Last 4 of SSN	DL / State ID	Bank Account	Bank Card	Medical Data
Grantee and Debtor Data									
Neighborly	**Budget** - Applications for ARPA and Community Agency grants; **CD** - Grant applications, loan applications, loan supporting documentation, and the Assistant Transmittal Form.	X	X	X	X	X	X		
Shared Drives	**Budget** - CIRC-RF Grant tax support records. **CD** - Grant supporting documentation and tenant applications. **BIA** - Loan supporting documentation. **DOT** - PL 104 (d) Planning Grant and STBG-DA State Reimbursements. Locally administered projects supporting documentation for reimbursements to subrecipients. **CMO** - Scanned Request for Check support.	X	X	X		X	X		X
Interoffice Mail - RICOH	**CD** - Loan setup documentation for single family housing sent to **Revenue.** Loan transmittal checklist sent to **Revenue**. **BIA** - Loan package documentation for setup sent to **Revenue** and **AP**. **DOT** - Signed paperwork and provisional forms sent to **AP.**	X	X	X			X		
Hardcopy in unsecured area.	**CD** - Assistant Transmittal Forms and loan supporting documentation in staffs' cubicle areas; single family loan documents in cubicle area; and single family loan documents in communal unsecured cabinets. Grant hardcopy printouts in cubicles and within communal unsecured cabinets.		X	X	X		X	X	
Hardcopy in unsecured mailbox.	**CD** - Assistant Transmittal Form in the Director's and staff's mailboxes; loan supporting documentation in staff mailbox; grant supporting documentation in the divisional supervisor's inbox; hardcopy grant folders in the communal area mailbox.		X	X	X	X	X	X	X
Outlook Emails	**BIA** - BIA receives loan applications, provides the loan committee a completed scanned loan package, and provides W9 amongst BIA staff, **AP**, and **Revenue**. **CD** - Tenant applications, grant supporting documents, and loan supporting documentation provided by applicants. **DOT** - Subrecipient reimbursement requests.	X	X	X	X	X	X		X

Controls Over PII - Grantee and Debtor Data		Sensitive PII							
Sensitive PII Repository (Location)	Type of Information/Data	TIN	SSN	DOB	Last 4 of SSN	DL / State ID	Bank Account	Bank Card	Medical Data
Debtor Data									
eWorks	**CD** - Request for a purchase order includes a loan applicant's Assistant Transmittal Form. **Budget** and **BIA** - New vendor/community agency includes their W9.	X			X				
Mortgage Servicer System	**Revenue** - Loan client information.	X	X	X					
OneDrive	**CD** - Loan applicant's Assistant Transmittal Form.				X				
Hardcopy in secured file room	**CD** - Loan files include Assistant Transmittal Forms; denied or cancelled loan applications; and single family loan documents. **Revenue** - Old notes, deeds, and old loan documentation.		X	X	X				
Hardcopy in secured staff office area.	**CD** - Pre-loan files, loan supporting documentation, and closing files.		X	X	X				
Hardcopy in secured mailbox.	**Revenue** - ACH mortgage payment supporting documentation.						X		
Hardcopy in unsecured area.	**Revenue** - ACH mortgage payment supporting documentation.						X		
Hardcopy in secured staff office area.	**Revenue** - IRS Reporting 1098-INT, 1099-A, or 1099-C printouts; old notes and deeds; and supporting loan documentation.	X	X						
Hardcopy in unsecured area.	**BIA** - Loan supporting documentation in unsecured communal file cabinets, workspace, and staff file cabinets; old loan documentation in City Hall basement cabinets.	X	X				X		

Sensitive Data Repositories Review

Partner Connect

Partner Connect is a program which provides resources, data, analysis, and support for the North Carolina Department of Transportation (NCDOT) professionals and stakeholders for transportation activities. The program is used by DOT management to fulfill grant activity parameters as NCDOT requires use of this electronic platform for grant reimbursements.

Sensitive Data Control Review

The Partner Connect program contains sensitive PII such as a subrecipient's TIN. This sensitive data's controls include login and password requirements.

Enterprise Business System (EBS) portal

NCDOT requires use of this electronic platform for DOT. The required grant reimbursement procedure entails supplying payment information such as invoices and supporting documentation provided by subrecipients – including proof of payment.

Sensitive Data Control Review
The EBS platform contains sensitive PII such as a subrecipient's TIN and bank account information. This sensitive data's controls include login and password requirements.

CMO Hard Drive
For the COVID-19 Response Fund for Forsyth County, the CMO's grant management activities required use of an office hard drive to store payment evidence through scanned copies of Request for Check Support – including proof of payment to grant subrecipients.

Sensitive Data Control Review
The CMO's hard drive contains sensitive PII such as a grant subrecipient's TIN. This sensitive data's controls include login and password requirements.

DOT Hardcopy Files in Unsecured Mailbox
The DOT office manages hardcopy files to support their varying grant processes. Hardcopy files serving as part of grant reimbursement support are kept by multiple DOT staff within their own unsecured mailboxes. In particular, hardcopy office area grant files are represented by hardcopy printouts for reimbursement in administrative secretary inbox. Further hardcopy provisional paperwork includes subrecipient reimbursement supporting documents which can be found in the mailboxes of the finance manager and the DOT Director, respectively.

Sensitive Data Control Review
The unsecured hardcopy files found within the DOT mailboxes contain sensitive PII such as SSN, TIN, and bank account information.

All of the hardcopy files with sensitive PII in the aforementioned areas are protected with security that includes a locked building supported by electric swipe pads; however, neither the individual DOT offices nor the mailboxes are secured within the building.

CMO Hardcopy Files in Unsecured Area
The CMO manages hardcopy files to support their grant contribution processes. Hardcopy files serving as part of grant support are kept within the CMO area. In particular, hardcopy office area grant files are represented by hardcopy printouts of grant applications and request for check support.

Sensitive Data Control Review
The unsecured hardcopy files found within the CMO area contain sensitive PII such as the grant applicant's TIN.

All of the hardcopy files with sensitive PII in the office area are protected with security that includes a locked building supported by electric swipe pads. Furthermore, the CMO suite door is locked at the end of the day, but the sensitive grant hardcopy materials are contained within an office that is not locked.

Neighborly
Neighborly is a cloud-based software used throughout the City's departments and divisions to replace paper-based applications, manual processes, and outdated technology to improve efficiency and regulatory compliance of housing, economic, and community development programs.

Budget uses Neighborly for management support related to funding of community agencies. Funding may come from grant monies associated with the American Rescue Plan Act (ARPA) or other grant resources.

CD uses Neighborly for management support related to the funding of various housing, economic, and community development programs. Both grant and loan applications are managed by CD within the platform. Furthermore, CD stores loan supporting documentation and assistant transmittal forms within Neighborly.

Sensitive Data Control Review
For Budget, the Neighborly platform maintains grant applicant information which contains sensitive PII such as the grantee's TIN.

For CD, the Neighborly platform maintains grant and loan application information which contains sensitive PII such as SSN, DOB, bank account information, DL, and the last four digits of the SSN.

This sensitive data's controls include login and password requirements.

Shared Drives
Many departments and divisions utilize shared drives to manage grant and/or loan supporting documentation for their varying processes. Budget uses their shared drive as part of management support for the Community Investment Review Committee Response Fund (CIRC-RF).

CD uses their shared drive as part of grants support of both documentation and tenant applications.

BIA uses their shared drive as part of management support of loan documentation.

DOT uses their shared drive to assist with managing grant activities associated with planning grants and state reimbursements and to help manage locally administered projects supporting documentation for reimbursements to subrecipients.

CMO uses their shared drive as part of support in managing scanned request for checks.

Sensitive Data Control Review
Per IS, usage of the network shared drive is encouraged since it is protected by the Microsoft Active Directory platform and policies.

The shared drive grantee information for Budget contains sensitive PII such as the grantee's TIN.

The shared drive grantee information for CD contains sensitive PII such as SSN, DOB, DL, and medical data.

The shared drive loan support information for BIA contains sensitive PII such as TIN, SSN, and bank account information.

The shared drive loan support information for DOT contains sensitive PII such as TIN and bank account information.

The shared drive grant support information for CMO contains sensitive PII such as the grantee's TIN.

Interoffice Mail - RICOH
Grant and loan documentation is sent via interoffice mail throughout the various departments and divisions within the City.

Interoffice mail sent from CD to Revenue includes both loan setup documentation for single family housing and loan transmittal checklists.

Interoffice mail sent from BIA to Revenue and AP includes loan package documentation for setup.

Interoffice mail sent from DOT to AP includes signed paperwork, provisional forms, and other grant documentation for reimbursement.

Sensitive Data Control Review
CD periodically sends sensitive interoffice mail to Revenue that contains sensitive PII such as SSN and DOB. BIA periodically sends sensitive interoffice mails to either Revenue or to AP that contains sensitive PII such as SSN, TIN, and DOB. DOT periodically sends sensitive interoffice mail to AP that contains sensitive PII such as SSN, TIN, and bank account information.

The various controls relating to RICOH, the vendor delivering interoffice mail, are as follows: 1) RICOH policy states RICOH employees will never open documents; 2) Any documents handled by RICOH are treated as confidential; 3) All RICOH employees are required to have background screenings, criminal background checks, drug tests, and online course training; 4) RICOH employees are provided a City employee badge; 5) All RICOH handled mail is locked in the employee's vehicle and secured till arrival at RICOH's main office in the Bryce Stewart building; and 6) All RICOH employees receive annual internal training on confidentiality.

<u>CD Hardcopy Files in Unsecured Area</u>
The CD office manages hardcopy files to support their grant and loan processes. Hardcopy files serving as part of grant support are kept within the CD office area. In particular, hardcopy office area grant files are represented by hardcopy printouts of grant materials in office cubicles and within communal unsecured cabinets. Loan materials include: assistant transmittal forms; loan support documentation in staffs' cubicle areas; and single family loan documents filed within communal unsecured cabinets.

Sensitive Data Control Review
The unsecured grant hardcopy files found within the CD office area contain sensitive PII such as SSN, the last four digits of the SSN, bank account information, and bank card information. The unsecured loan hardcopy files found within the CD office area contain sensitive PII such as SSN, DOB, and the last four digits of the SSN.

All of the hardcopy files with sensitive PII in the office areas are protected with security that includes a locked building supported by electric swipe pads; moreover, the CD office suite door is locked at the end of the day. Non-CD individuals are not allowed in the communal area without a chaperone. However, the aforementioned sensitive grant and loan hardcopy materials are not secured as the communal cabinets are not locked nor are some of the associated staff cubicle drawers within the office.

<u>CD Hardcopy Files in Unsecured Mailbox</u>
The CD office manages hardcopy files to support their varying grant processes. Hardcopy files serving as part of grant supporting documentation can be found in the divisional supervisor's inbox. Hardcopy grant folders are kept in the communal area mailbox for the Director to review and approve. Regarding loan activities, office area loan files are represented by hardcopy printouts of assistant transmittal forms in the Director's and staffs' mailboxes, and other supporting hardcopy loan documentation in staffs' mailboxes.

Sensitive Data Control Review
The unsecured hardcopy grant files found within CD mailboxes contain sensitive PII such as SSN, the last four digits of the SSN, DOB, DL, bank account information, bank card information, and medical data. The

unsecured hardcopy loan files found within CD mailboxes contain sensitive PII such as the last four digits of the SSN.

All of the hardcopy files with sensitive PII in CD mailboxes are protected with security that includes a locked building supported by electric swipe pads; moreover, the CD office suite door is locked at the end of the day. Non-CD individuals are not allowed in the communal area without a chaperone. However, the aforementioned sensitive grant and loan hardcopy materials are not secured within the mailboxes as they are within the communal area.

Microsoft Outlook Emails

Microsoft Outlook is the City's chosen method for sending emails that include sensitive records with PII. Microsoft Outlook emails sent from BIA to other BIA staff, loan committee members, AP, and Revenue personnel include an applicants' W9.

Microsoft Outlook emails sent from grantees to CD include the grantees' application and supporting documentation. Outlook emails sent from loan applicants to CD contain loan supporting documents.

Emails from grant subrecipients to DOT staff (and emails shared amongst DOT staff) include subrecipient reimbursement materials.

Sensitive Data Control Review

Microsoft Outlook emails from BIA to other BIA staff, loan committee members, AP, and Revenue personnel can contain sensitive data as SSN, TIN, and bank account information.

Emails from grantees to CD can contain SSN, DOB, DL, bank account information, and medical data.

Emails from loan applicants to CD can contain SSN, DOB, and the last four digits of the SSN.

Emails from grant subrecipients to DOT staff (and emails shared amongst DOT staff) can contain sensitive data as SSN, TIN, and bank account information.

Controls relating to accessing this sensitive data include login and password requirements. Moreover, Microsoft Outlook emails sent solely on City servers are encrypted.

eWorks

eWorks is a workflow management system framework. The currently developed workflows consist of business process requests routed through City department/divisions' management approvals based on business rules.

CD uses eWorks as part of their loan process as CD's request for purchase order procedure includes attaching a loan applicant's assistant transmittal form.

As part of a grant process for Budget and as part of a loan process for BIA, a new grantee or debtor's W9 is attached within eWorks to establish the new entity as a recognized vendor.

Sensitive Data Control Review

CD's inclusion of a loan applicant's assistant transmittal form within eWorks contains sensitive PII such as the last four digits of the SSN.

The Budget and BIAs' processes which attach a new entity's W9 within eWorks contain sensitive PII such as TIN.

Access to eWorks in general is controlled by a user account and password. Once inside of eWorks, there are additional layers of security associated with specific workflows depending upon the role and level of security assigned. In particular, the only departments and divisions allowed to access specific eWorks items are Purchasing, AP, Internal Audit, the originating department requester and approvers, and City management approvers.

Mortgage Servicer System

Revenue is responsible for servicing all loans from the City to outside entities. After loans are closed, loan packages are sent to Revenue from CD and BIA. The system application used by Revenue is Mortgage Servicer. This system maintains the new electronic loan files which contain debtor information.

Sensitive Data Control Review

Mortgage Servicer contains sensitive PII such as TIN, SSN, and DOB. This sensitive data's controls include login and password requirements.

OneDrive

CD periodically uses OneDrive as it enables staff members to securely share loan materials and it controls levels of security via direct access or links for viewing files.

Sensitive Data Control Review

OneDrive contains sensitive PII such as the last four digits of the SSN. This sensitive data's controls include login and password requirements.

Hardcopy Files in Secured File Room

CD manages hardcopy files to support their varying loan processes. Hardcopy files serving as part of loan support such as assistant transmittal forms, denied or cancelled loan applications, and single family loan documents are kept in a secure file room.

Revenue also manages hardcopy files to support their loan processes. Hardcopy files serving as part of loan support includes old notes, deeds, and old loan documentation kept in a secure file room.

Sensitive Data Control Review

CD and Revenue security includes electric key pads as well as electric swipe pads to secure entry and exit from the Bryce A. Stuart (BAS) Municipal Building. The secured hardcopy files found within the CD file room are secured by electric key pads and contain sensitive PII such as SSN, DOB, and the last four digits of the SSN.

The secured hardcopy files found within the Revenue file room are secured by electric swipe pads and contain sensitive PII such as SSN.

CD Hardcopy Files in Secured Staff Office Area

CD's office area hardcopy files such as pre-loan files, loan supporting documentation, and closing files are kept in staffs' locked drawers.

Sensitive Data Control Review

The secured hardcopy files found within the CD staff's locked drawers contain sensitive PII such as SSN, DOB, and the last four digits of the SSN.

Revenue Hardcopy Files in Secured Mailbox

Revenue's hardcopy files associated with loan activity and in particular ACH mortgage payment supporting documentation are initially delivered into a secure mailbox within Revenue.

Sensitive Data Control Review

The secured hardcopy files found within the Revenue mailbox room are secured by electric swipe pads and contain sensitive PII such as bank account information.

Revenue Hardcopy Files in Unsecured Area

Revenue manages hardcopy files to support their loan processes. These files are kept within the Revenue office area. In particular, hardcopy office area loan files are represented by ACH mortgage payment supporting documentation which can be found within unsecured office cubicles.

Sensitive Data Control Review

The unsecured loan hardcopy files found within the Revenue office area contain sensitive PII such as bank account information.

All of the hardcopy files with sensitive PII in the office areas are protected with security that includes a locked building supported by electric swipe pads; moreover, the Revenue office suite door is locked at the end of the day and non-Revenue individuals are not allowed in the secured area without a chaperone. However, the aforementioned sensitive loan hardcopy materials are not secured nor are some of the associated staff cubicle drawers locked within particular office areas.

Revenue Hardcopy Files in Secured Staff Office Area

Revenue's office area hardcopy files such as IRS Reporting 1098-INT, 1099-A, or 1099-C printouts and old notes and deeds are kept in the secured staff office area. Moreover, older supporting loan documentation is kept in locked storage in the BAS basement.

Sensitive Data Control Review

Electric swipe pads secure hardcopy files found within both the Revenue office area and in the BAS basement and contain sensitive PII such as SSN and TIN.

BIA Hardcopy Files in Unsecured Area

BIA manages hardcopy files to support their loan processes; these files are kept within the BIA office area. In particular, hardcopy office area loan files are represented by loan supporting documentation in unsecured communal file cabinets, in unsecured workspaces, and in unsecured staff file cabinets. Furthermore, old loan documentation can be found unsecured in City Hall basement cabinets.

Sensitive Data Control Review

The unsecured loan hardcopy files found within both the BIA office area and City Hall basement contain sensitive PII such as TIN, SSN, and bank account.

All of the hardcopy files with sensitive PII in the office areas are protected with security that includes a locked building supported by electric swipe pads; however, the BIA office suite door is not locked at the end of the day. Consequently, the aforementioned sensitive loan hardcopy materials are not secured nor are the associated staff cubicle drawers, file cabinets within BIA office, and associated file cabinets within the City Hall basement areas locked.

Other Observations

The City Council Resolution dated October 27, 2008 authorized the creation of the City's Identity Theft Prevention Program (Red Flag Program) to comply with the guidelines set forth in the Fair and Accurate Credit Transactions Act of 2003. Internal Audit inquired regarding the Identity Theft Prevention Program during the current review on grantee and debtor PII Data. Internal Audit's review determined that the City has not implemented this program. There are no known City-wide policies for the designation and protection of PII nor policies for evaluating the confidentiality of PII. Furthermore, the City does not have a policy in place covering sensitive PII data retention; such a policy may provide guidance as to the treatment of sensitive PII emails (i.e. email management and removal). However, IS has indicated a City-wide policy for both the designation and protection of PII will be drafted and recommended to the City Manager's Office. The policy will cover sensitive PII data retention and provide guidance as to the treatment of sensitive PII data within email. The activities and policies related to PII data will be closely associated with the City's Cybersecurity Program. During the review, it was recognized that IS has implemented and continues to enhance proactive procedures that address PII specifically and cybersecurity across the organization.

IS activities address employee training for prevention and awareness that include: strong passwords; confidential information sharing; end point security; security of printouts; locking computer devices; multi-factor authentication (MFA); reporting suspicious behavior and emails, attachments, links, etc.; employee awareness via email; intranet postings on the Employee Home Center; awareness posters displayed in City facilities; and information shared with the IS Liaison community. Earlier this fiscal year, IS initiated a new on-line employee cybersecurity training program. To date approximately 55% of all City employees have completed the on-line training program.

Although not all PII has been identified in the organization, IS has established internal phishing campaigns for all City employees that include 'baited' emails that invite and entice the employee to click on a link or attachment. The goal of the phishing campaigns is not to identify employees that 'took the hook' in an email in a negative sense, but rather to help educate the employee and promote cyber awareness. When an employee clicks on a 'baited' attachment or link, an educational splash page is displayed to help the employee understand how he or she could have identified the email as phishing and avoided clicking on the bait. IS' first phishing campaign in September 2021 using the current software tools resulted in an employee click rate of 31%; the March 2022 campaign had a click rate of 2.3%. Per cybersecurity vendors and insurance providers, the industry average phishing click rate is 3.26%. IS staff is currently working on the creation of phishing campaigns designed specifically for PII data and the users of such data.

Discussions and expectations between management and the Chief Information Officer (CIO) have confirmed that the CIO continues in the role of the Program Coordinator. As part of the FY20-21 Work Plan, IS initiated a program to identify all data stored in their data bases and files that can be classified as either obvious or potential PII data. For over twenty years, IS has maintained an index of all of the City's data bases and system files. This documentation is maintained in part as a response to North Carolina Public Records laws and the frequent requests from the public for information within the guidelines of these laws. IS staff continues to add improvements to the documentation and record keeping; PII data is a focal point. This includes categorizing the various data bases and files in terms of a level of risk, documenting why and how specific PII data is required for business operations, and how it is protected.

In the event of a compromise to any data base or file, staff would follow operational Incident Response Plans.

The National Institute of Standards and Technology's (NIST) Guide to Protecting the Confidentiality of PII lists several recommendations to effectively protect PII (*NIST 800-122*). NIST recommends that organizations:

- Identify all the PII residing in that organization (priority: sensitive PII);
- Minimize the use, collection, and retention of PII to what is strictly necessary;
- Categorize PII (level of impact on confidentiality);
- Safeguard PII based on impact to confidentiality. Safeguards for protecting PII include:
    - Policies and procedures
    - Training
    - Good security practices
- Encourage close coordination within the organization.

****

Respectfully submitted,

Heather Smith
Internal Audit Administrator

Paul Sherman
Internal Auditor

Distribution
Lee Garrity
Aaron King
Ben Rowe
Johnnie Taylor
Patrice Toney
Marla Newman
Sharon Richmond
Meridith Martin
Sarah Coffey
Toneq' McCullough
Brenda King
Ken Millet
Lisa Saunders
Kelly Latham
Larissa Mathis
Tom Kureczka
Scott Tesh