CITY OF WINSTON-SALEM CONTROLS OVER PERSONAL IDENTIFYING INFORMATION – CRIME AND VICTIM DATA REVIEW

Submitted by:
Office of Performance and Accountability
Internal Audit Division
April 2021

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, and Revenue), Human Resources, Community Development, Business Inclusion and Advancement, 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 (I.S.) 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 will have 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), passports or foreign IDs, bank account information, bank card information, PINS, user IDs and passwords, and latent prints (includes fingerprints); moreover, the following PII can also be considered sensitive (medical information, 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.

The City's Police Department collects sensitive PII from both employees and citizens. This sensitive PII data can be collected in person and electronically. The Police Department has multiple general orders (GOs) and divisional standard operating procedures (SOPs) which serve as controls to the protection of sensitive PII. The performance of everyday police activities may require the Police Department to transmit PII and the data may be retained by cloud services or other application service providers. The Police Department bureaus and divisions have common process requirements, shared system applications, shared databases, their own hardcopy files, and their own set of PII.

Scope of Review Procedures Performed

Off-site interviews of Police Department staff were performed during October-December 2020. 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 the Police Department bureaus and divisions were then evaluated for significant vulnerabilities.

The following chart outlines the Sensitive PII Repositories found:

Controls Over PII - Crime and Victim Data Review		Sensitive PII								
Sensitive PII Repository (Location)	**Type of Information/Data**	**SSN**	**DOB**	**Last 4 of SSN**	**DL / State ID**	**Passport or Foreign ID**	**Bank Account**	**Bank Card**	**Latent Prints**	**Medical Data**
Below Repositories Used By All Police Bureaus/Divisions--Unless Otherwise Designated.										
Application Extender	Investigative Services Bureau (ISB) Forensic Services Division (FSD) field notes, latent prints, and electronic documentation.*	X	X	X	X	X	X	X	X	
Division of Criminal Information and National Crime Information Center (DCI/NCIC)	Crime data maintained by Criminal Justice Information Services (CJIS). **	X	X	X	X					
Evidence.com	Evidence database retains photos, videos, and fieldnotes. ***	X	X	X	X				X	
PowerDMS	Minimal supporting documentation. ****	X	X	X						
Evidence collected	Evidence/materials collected. *****	X	X	X	X	X	X	X		
Hardcopy in office area.	To Be Shredded material	X	X	X	X	X	X	X	X	X
RMS	Field notes, latent prints, and electronic documentation.	X	X	X	X	X	X	X	X	
Hardcopy in secured storage area at Alexander R. Beaty Public Safety Training & Support Center	**ISB FSD** - Historical photographs, negatives, and latent print card materials. **Support Services Division (SSD) Records** - Archived records of homicides, death investigations, and fatalities. **Office of the Chief of Police (OCP) Professional Standards Division (PSD)** - Archived records of supporting prior investigations. **OCP Public Safety Attorney (PSA)** - Archived files.	X	X	X	X	X	X	X	X	
Dropbox	**SSD Records** - Sensitive records/reports. **OCP PSA** - Sensitive records.	X	X	X	X	X	X	X	X	
Hightail Emails	**SSD Records** - Sensitive records. **OCP PSA** - Sensitive records.	X	X	X	X	X	X	X	X	
Interoffice Mail - RICOH	**ISB FSD** - Evidence. **Note:** All other Police areas send interoffice mail without sensitive data included.	X	X	X	X	X	X	X		
Outlook Emails	**OCP PSA** - Documentation (to police personnel). **ISB FSD** - Documentation. (**Only DOB**). **Note:** All other Police areas send emails but without sensitive data being included.	X	X	X	X	X	X			

Sensitive PII Repository (Location)	Type of Information/Data	SSN	DOB	Last 4 of SSN	DL / State ID	Passport or Foreign ID	Bank Account	Bank Card	Latent Prints	Medical Data
Hardcopy in Criminal Investigations Division (CID) office area	Case file support documentation	X	X	X						
Hardcopy in FSD office area	Photo-labs' photographs and prints; officers' field notes documentation; expungement order; and citizen/applicant file documentation	X	X	X	X	X	X	X		
Hardcopy in Detention Center	**ISB FSD** - Latent prints and finger print card documentation	X	X	X					X	
	ISB FSD - DNA sample ID card documentation		X							
Hardcopy in Detention Center in Storage Room.	**ISB FSD** - Breath Test and related report documentation		X		X					
Hardcopy in Detention Center in Common Area.	**ISB FSD** - Breath Test and blood draw related report documentation		X		X					
Hardcopy for Special Operations Division (SOD) Gang Unit in office area.	Officers' Field Notes documentation.		X							
Hardcopy for SOD Gang Unit in patrol cars.	Officers' Field Notes documentation.		X							
Hardcopy in Evidence Management (EM) area.	Support documentation for all evidence.		X							
Hardcopy in the IT office area.	Documentation relating to projects for support. Police reports (customized crystal reports).	X	X	X	X		X	X		
Hardcopy in Records office area.	Hardcopy records of homicides, death investigations, missing persons, and fatalities.	X	X	X	X	X	X	X	X	
Hardcopy in PSD area.	Hardcopy/video records and other supporting materials.		X		X		X	X		
Hardcopy in PSA office area	Hardcopy expungement requests; Record's/FSD photographs for court order requests; documentation for reviewing officer actions; and documentation for citizen concerns.		X		X		X			X
Checks issued for Special Investigations Division (SID)	Checks issued/distributed to officers to finance various operations.						X			

*Note: for crime and victim data, used by ISB's FSD, Operations Support Division's (OSD) EM, SSD's IT and Records.

**Note: for crime and victim data, used by ISB's FSD, OSD's EM, and SSD's IT.

***Note: for crime and victim data, used by CID, ISB's FSD, SOD's SWAT and DWI, SSD's IT, OCP's PSD and PSA.

****Note: for crime and victim data, used by ISB's FSD, SSD's IT, and OSD's EM

*****Note: for crime and victim data, used by SOD's Canine Services Unit, DWI, and the Gang Unit.

Sensitive Data Repositories Review

Application Extender Database

Application Extender is a record management system used throughout the Police Department to retain forensic field notes, latent prints, and electronic documentation. **Note:** for crime and victim data, this

database is used by the following areas within the Police Department: Investigative Services Bureau's (ISB) Forensic Services Division (FSD), Operations Support Division's (OSD) Evidence Management (EM), Support Services Division's (SSD) Information & Technology (IT) and Records.

Sensitive Data Control Review

The Application Extender database contains sensitive PII such as SSN, DOB, last four of SSN, DL, passports or foreign IDs, bank account information, bank card information, and latent prints. This collection of data is in a server database within the Police Information and Technology (IT) datacenter and thereby follows standard IT Server security protocols. This sensitive data's controls include login and password requirements as well as the following Police GO and SOPs: GO 1.25 – Dissemination of Information; GO 4.05 – Criminal Intelligence; SOP 1.0 Quality Manual; SOP 3.0 Administrative Manual; SOP 6.0 Friction Ridge Examination Manual; and SOP 7.0 Police Processing Manual.

Division of Criminal Information and National Crime Information Center (DCI/NCIC) Database

The DCI/NCIC database serves as an information sharing tool for crime data maintained by the FBI which is used throughout the Police Department. **Note:** for crime and victim data, this database is used by the following areas within the Police Department: ISB's FSD, OSD's EM, and SSD's IT.

Sensitive Data Control Review

The DCI/NCIC database contains sensitive PII such as SSN, DOB, last four of SSN, and DL. This database is accessed through a secure connection and thereby follows FBI's security protocols. This sensitive data's controls include data and connection encryption. Access requires sworn or unsworn officers to pass certifications in order to gain access to different levels of the database. Police divisions may release information to officers but there is a protocol requiring an access form to be completed and approved. Further controls relating to accessing this sensitive data include login and password requirements as well as the following Police GOs and SOP: GO 1.25 – Dissemination of Information; GO 4.05 – Criminal Intelligence; and SOP 1.0 Quality Manual.

Evidence.com Database

Evidence.com is a secure cloud-based evidence database used throughout the Police Department to retain photos, videos, and field notes. This database allows for the ability to create 'cases' where direct access of only specified/relevant materials can be provided to specified individuals. Note: for crime and victim data, this database is used by the following areas within the Police Department: Criminal Investigations Division (CID), ISB's FSD, Special Operations Division's (SOD) SWAT and Forsyth County Driving While Impaired (DWI) Task Force, SSD's IT, Office of Chief of Police's (OCP) Professional Standards Division (PSD), and Public Safety Attorney (PSA).

Sensitive Data Control Review

The Evidence.com database contains sensitive PII such as SSN, DOB, last four of SSN, DL, and latent prints. This collection of data is maintained as a cloud-based system which accesses the Police Department's information and thereby follows standard IT Server security protocols as it uses an encrypted connection. The database allows for time stamping for when sent, delivered, and accessed. This particular advantage mitigates any concerns for a receiver to state that they didn't receive an item as evidence.com can confirm delivery. Moreover, sensitive work product such as created by PSD can be secured on their own separate server. This sensitive data's controls include login and password requirements as well as the following Police GOs: GO 1.25 – Dissemination of Information and GO 4.05 – Criminal Intelligence.

PowerDMS Database

PowerDMS is a secure search engine and database used throughout the Police Department to retain Police policies and procedures and other supporting documentation. Note: for crime and victim data, this database is used by the following areas within the Police Department: ISB's FSD, SSD's IT, and OSD's EM.

Sensitive Data Control Review

The PowerDMS database contains sensitive PII as SSN, DOB, and the last four of SSN. It is hosted on a cloud-based server and follows standard IT Server security protocols. This database allows for restrictions on cases in order to limit to particular Police Department personnel. This sensitive data's controls include login and password requirements as well as the following Police GOs and SOPs: GO 1.25 – Dissemination of Information; GO 4.05 – Criminal Intelligence; SOP 1.0 Quality Manual; SOP 3.0 Administrative Manual; SOP 6.0 Friction Ridge Examination Manual; and SOP 7.0 Police Processing Manual.

Evidence Collected

For crime and victim data, SOD's Canine Services Unit, DWI, and the Gang Unit all collect evidence during the course of operations. This evidence is submitted to EM.

Sensitive Data Control Review

Evidence collected from SOD's Canine Services Unit, DWI, and the Gang Unit can contain sensitive PII such as SSN, DOB, last four of SSN, DL, passports or foreign IDs, bank account information, and bank card information. The controls relating to accessing this sensitive data include the following Police GOs: GO 1.25 – Dissemination of Information and GO 4.05 – Criminal Intelligence. Other controls include both Commission on Accreditation for Law Enforcement Agencies (CALEA) and CJIS standards.

Hardcopy Files in Office Areas – To be Shredded

Hardcopy files to be shredded are securely kept throughout the Police Department. The department uses the vendor Shred-IT.

Sensitive Data Control Review

The securely stored hardcopy files contain sensitive PII such as SSN, DOB, last four of SSN, DL, passports or foreign IDs, bank account information, bank card information, latent prints, and medical information. All of the hardcopy files to be shredded are kept in locked bins; the Police bureau/division supervisor maintains a key for these locked bins. It is the practice for Police personnel to accompany the Shred-IT employee to the shredding vehicle on-site and witness the actual shred process of the designated 'to be shredded' material. Once the shredding has been completed, the designated Police personnel receives a certificate of destruction. Security for each Police office area is protected by electric swipe pads and key locks to secure entry and exit. Further controls relating to accessing this sensitive data include the following Police GOs: GO 1.25 – Dissemination of Information and GO 4.05 – Criminal Intelligence. Depending on the Police bureau or division, there are likely further SOPs relating to Division Security which serve as controls of hardcopy file destruction.

RMS Database

This database is a record management system which allows the Police to retain various records, field notes, latent prints, and other electronic documentation. RMS is a secure database used throughout the Police Department.

Sensitive Data Control Review

The RMS database contains sensitive PII such as SSN, DOB, last four of SSN, DL, passports or foreign IDs, bank account information, bank card information, and latent prints. It is maintained on a Server within the Police IT datacenter and thereby follows standard IT Server security protocols; the server housing RMS records is onsite with off-site backups over an encrypted connection. This database allows for restrictions on cases in order to limit to particular Police personnel. This sensitive data's controls include login and password requirements as well as the following Police GOs and SOPs: GO 1.25 – Dissemination of Information; GO 4.05 – Criminal Intelligence; SOP 1.0 Quality Manual; SOP 3.0 Administrative Manual; SOP 6.0 Friction Ridge Examination Manual; and SOP 7.0 Police Processing Manual.

Hardcopy Files in Secured Storage Area

Police Department hardcopy files are securely stored at the Beaty Public Safety Training and Support Center (Beaty). Note: for crime and victim data, the secured storing of hardcopy files is used by the following areas within the Police Department: 1) ISB's Forensics - Historical photographs, negatives, and latent print card materials; 2) SSD's Records - Archived records of homicides, death investigations, and fatalities; 3) OCP's PSD - Archived records supporting prior investigations; and 4) OCP's PSA - Archived files.

Sensitive Data Control Review

The securely stored hardcopy files contain sensitive PII such as SSN, DOB, last four of SSN, DL, passports or foreign IDs, bank account information, bank card information, and latent prints. All of the hardcopy files are kept in the Police bureau/division designated and separately fenced storage areas at Beaty. Security includes electric swipe pads as well as key locks to secure entry and exit from Beaty. Further controls relating to accessing this sensitive data include the following Police GOs: GO 1.25 – Dissemination of Information and GO 4.05 – Criminal Intelligence.

Dropbox

Dropbox is an electronic folder created on a separate computer drive that only specified individuals can access. A dropbox is usually organized to send copies of reports being sent from Records to other areas. **Note:** for crime and victim data, this information sharing technique is only used by the following areas within the Police Department: 1) SSD's Records – where sensitive record requests are met by sending copies of reports to Police personnel via Dropbox.; and 2) OCP's PSA – where sensitive record requests are also met via Dropbox.

Sensitive Data Control Review

Dropbox contains sensitive PII such as SSN, DOB, last four of SSN, DL, passports or foreign IDs, bank account information, bank card information, and latent prints. This information sharing technique is only accessible to select persons. Further controls relating to accessing this sensitive data include login and password requirements as well as the following Police GOs: GO 1.25 – Dissemination of Information; GO 1.51 – Electronic Messaging and City Phone Use; and GO 4.05 – Criminal Intelligence.

Hightail Email

Hightail email is the Police Department's chosen encryption method for sending emails which include sensitive records with PII. Sensitive record requests are sent via the Hightail email system to meet Criminal Justice Information Services (CJIS) standards. Records uses Hightail to further include restrictions and limits establishing how long and for whom information is specified. **Note:** for crime and victim data,

this encrypted email method is only used by the following areas within the Police Department: 1) SSD's (Records); and 2) OCP's PSA.

Sensitive Data Control Review

Hightail emails can contain sensitive PII such as SSN, DOB, last four of SSN, DL, passports or foreign IDs, bank account information, bank card information, and latent prints. This information sharing technique is required by Police IT in order to meet CJIS encryption standards. A sender can further add additional passwords for access to a Hightail email. The recipient only can open the Hightail email with the credentials that are communicated by the sender for a limited time period. Further controls relating to accessing this sensitive data include login and password requirements as well as the following Police GOs: GO 1.25 – Dissemination of Information; GO 1.51 – Electronic Messaging and City Phone Use; and GO 4.05 – Criminal Intelligence. Another control relates to NCGS 132-1.4 - Criminal Investigation and Intelligence Records.

<u>Interoffice Mail - RICOH</u>

Police documentation is sent via interoffice mail throughout the various Police bureaus/divisions and City departments/divisions. **Note:** this mail method is used by all Police bureaus and divisions; however, for crime and victim data, ISB's Forensic Services Division (FSD) is the only Police division which chooses to send sensitive data (evidence for FSD) via Interoffice Mail.

Sensitive Data Control Review

FSD's sensitive interoffice mails are periodically sent to OSD's Judicial Services Unit FSD's interoffice mails with Police evidence contain sensitive PII such as SSN, DOB, last four of SSN, DL, passports or foreign IDs, bank account information, and bank card information. These FSD evidence mailings are only meant for the Judicial Services Unit operating out of the courthouse; however, FSD's interoffice mail route to the Judicial Service Unit includes a 'stopover' at the Vivian H. Burke Public Safety Center's general mail reception/inbox area. Although interoffice mail left in the Police Department's general mail reception is secure from the public, there is the potential risk for this evidence to be diverted within this multi-bureau/division inbox area; therefore, there is a potential concern for any evidence during the 'stopover' portion of the mail route. Internal Audit recommends the risks involved with FSD's interoffice mailing of sensitive evidence be mitigated by ensuring a more direct route to Judicial Services.

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 fingerprinted; 5) RICOH employees are provided a City employee badge; 6) RICOH employees receive a separate access badge after being independently vetted by EM; 7) 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 8) All RICOH employees receive annual internal training on confidentiality.

Further controls relating to accessing this sensitive data include the following Police GOs and SOPs: GO 1.25 – Dissemination of Information; GO 4.05 – Criminal Intelligence; SOP 1.0 Quality Manual, and SOP 7.0 Police Processing Manual. Other controls include both CALEA and CJIS standards.

Microsoft Outlook Emails

Microsoft Outlook is the Police Department's chosen method for sending emails that include sensitive records with PII within the City. Microsoft Outlook emails sent solely on City servers are encrypted—just not to CJIS security standards. **Note:** this email method is used by all Police bureaus and divisions; however, for crime and victim data, OCP's PSA and ISB's FSD are the only groups which choose to send sensitive data via Microsoft Outlook. OCP's PSA only emails sensitive data to Police personnel. ISB's FSD only emails sensitive data to the court system or to detectives.

Sensitive Data Control Review

Microsoft Outlook emails from OCP's PSA to Police personnel can contain sensitive data as DOB, DL, bank account information, and medical information. Emails from ISB's Forensics to the court system or to detectives contain DOB. Controls relating to accessing this sensitive data include login and password requirements as well as the following Police GOs: GO 1.25 – Dissemination of Information and GO 1.51 – Electronic Messaging and City Phone Use. Other controls include both CALEA and CJIS standards.

Hardcopy Files

Many Police bureaus/divisions manage hardcopy files to support their varying processes. Hardcopy files serving as part of case file support are kept by ISB's CID within their office area. Hardcopy office area files for ISB's FSD are represented by their photo lab's photographs and prints, officers' field notes, expungement orders, and both citizen and position applicant documentation. FSD also retains hardcopy files of latent prints, fingerprint card documentation, and DNA sample ID cards at their office area within the detention center. Further FSD's hardcopy of breath test and blood draw support documentation is kept within the storage room and common area of the detention center, respectively.

The SOD's Gang Unit retains hardcopy files of officers' field notes both in their office area and within their patrol cars.

OSD's EM manages a paper filing system that includes hardcopy files supporting all pieces of evidence within their office area.

The SSD's IT retains hardcopy files relating to project support. SSD's Records also keeps hardcopy files related to records of homicides, death investigations, missing persons, and fatalities within the Records office area.

OCP's PSD retains hardcopy files relating to records supporting investigations within their office area. OCP's PSA has hardcopy files for a number of varying reasons including: expungement requests; photographs (from Record's/Forensics) for court order case requests; officer action reviews; and citizen concerns documentation within their office area.

Sensitive Data Control Review

The securely stored hardcopy files for ISB's CID contain sensitive PII such as SSN, DOB, and last four of SSN. Securely stored hardcopy files for ISB's FSD contain sensitive PII as many contain SSN, DOB, last four of SSN, DL, passports or foreign IDs, bank account information, bank card information, and latent prints; the amount of sensitive PII varies depending on the activity and the required FSD support documentation.

SOD's Gang Unit and OSD's EM hardcopy files only contain the sensitive PII DOB.

SSD's IT hardcopy files include the sensitive PII SSN, DOB, last four of SSN, DL, bank account information, and bank card information; SSD's Records hardcopy files include all of IT's sensitive PII as well as passports or foreign IDs, and latent prints.

OCP's PSD hardcopy files contain sensitive PII including DOB, DL, bank account information, and bank card information. OCP's PSA hardcopy files contain sensitive PII including DOB, DL, bank account information, and medical information.

All of the hardcopy files with sensitive PII in the aforementioned areas are protected with security that includes locked offices, electric swipe pads, and key locks to secure entry and exit from each of these areas. Further controls relating to accessing this sensitive data include the following Police GOs: GO 1.25 – Dissemination of Information; GO 2.35 – Body Worn Recording Equipment; and GO 4.05 – Criminal Intelligence. Also, SOP controls for FSD include: SOP 1.0 Quality Manual; SOP 3.0 Administrative Manual; SOP 6.0 Friction Ridge Examination Manual; and SOP 7.0 Police Processing Manual. SOP controls for Records include: SOP 1.10 – Division Security; SOP 2.02 – Release of Complaint Reports; SOP 2.03 – Public Record Requests; and SOP 4.02 – Law Enforcement Service Request Form. For PSD other controls include NCGS Body Worn Camera Laws. For PSA further controls include: NCGS 130a which governs confidentiality of medical information and NCGS 132-1.4 which governs criminal investigation and intelligence records. Other controls include CALEA and CJIS standards.

Checks Issued for SID

Checks are periodically issued by the City's Finance Department for various operations managed by SID personnel.

Sensitive Data Control Review

The checks issued to SID personnel include the sensitive PII bank account information as they contain checking account and routing information. The checks are kept by SID personnel until they are cashed to fund operations. The sensitive data's controls include the following Police GOs: GO 1.25 – Dissemination of Information and GO 4.05 – Criminal Intelligence.

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 crime and victim 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. However, during the audit, it was recognized that I.S. is implementing proactive procedures in place that address both cybersecurity and PII.

I.S. activities include employee training for prevention and awareness that include: strong passwords; confidential information sharing; end point security; security of printouts; locking computer devices; reporting suspicious behavior and emails, attachments, links, etc.; employee awareness via email; intranet postings; awareness posters displayed in City facilities; and information shared with the I.S. Liaison community.

Although not all PII has been identified in the organization, I.S. has completed a first-pass review of all PII data within the business systems supported by I.S. Moreover, 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 their FY20-21 Work Plan, I.S. has initiated a project to proceed forward from the results of the first-pass review of all PII data. The results of the first-pass review will be evaluated to ensure any additional data from databases, current systems, enhanced systems, and new applications systems are part of this project. The project will also specifically address improvements as identified, such as the need for further documentation as to why and how specific PII data is required for business operations, how it is protected, and what mediation plans are in place should the data be compromised.

I.S. will also be drafting and recommending a City-wide policy to the City Manager's Office for both the designation and protection of PII. 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.

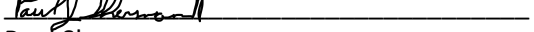
The National Institute of Standards and Technology's (NIST) Guide to Protecting the Confidentiality of PII lists several recommendations to effectively protect PII (*NIST 800-122*). NIST recommends that organizations:

- 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
Tasha Logan Ford
Police Chief Catrina Thompson
Tom Kureczka
Ben Rowe
Scott Tesh