Department of Legislative Services
Office of Legislative Audits

Personally Identifiable Information (PII) Audit Issues

Presentation to Joint Audit and Evaluation Committee

Gregory A. Hook, CPA
Stephen P. Jersey, CPA, CISA

December 17, 2019

Presentation Overview

Today's presentation on PII issues identified in OLA audit reports issued since fiscal year 2014 will focus on the following information elements:

- Definition of PII Data
- State PII Security Requirements
- PII Within State IT Systems
- Volume of PII Records Within State Systems
- PII Data Security Risks
- OLA Audit PII Findings
- Conclusions
- Recommendations

Overview – PII Definition – Federal Government

The U.S. Department of Commerce's National Institute of Standards and Technology (NIST) defines PII as "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."

Examples of PII data per NIST's *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) (SP 800-112)* also include, but are not limited to:

- driver's license number, taxpayer identification number, or financial account or credit card number;
- street address or email address; and
- personal characteristics, including photographic image, fingerprints, handwriting, or other biometric data (such as retina scan, voice signature, or facial geometric pattern).

Overview – PII Definition – State of Maryland

Maryland PII definition found in two statutes:

State Government Article, Sections 10-1301 to 10-1308 considers PII to be an individual's first name or first initial and last name, personal mark, or unique biometric or genetic print or image, in combination with one or more of the following data elements:

1. Social Security number;
2. Driver's license number, state identification card number, or other individual identification number issued by a unit;
3. Passport number or other identification number issued by the United States government;
4. Individual Taxpayer Identification Number; or
5. Financial or other account number, a credit card number, or a debit card number that, in combination with any required security code, access code, or password, that would permit access to an individual's account.

Overview – PII Definition – State of Maryland (cont.)

In addition to the aforementioned State Government Article, the Commercial Law Article, Title 14, Subtitle 35 – (from the Maryland Personal Information Protection Act) also defines PII. This definition includes an individual's name and the same data elements as defined by State Government Article 10-1301, with the additional data combinations of:

1. health information, including information about an individual's mental health; or

2. a health insurance policy or certificate number or health insurance subscriber identification number, in combination with a unique identifier used by an insurer or an employer that is self-insured, that permits access to an individual's health information.

Background – PII - State Security Requirements

Multiple State IT Security Policies, depending upon the governmental area, address PII data protection.

- State of Maryland Information Technology Security Manual - published by DoIT – applies to State Executive Department and independent agencies
- USM IT Security Standards (Section III – Confidential Data)
- Administrative Office of the Courts – Judicial Information Systems – Information Security Policy (Sections 3.2 – Data Classification and 13 – Data Loss Prevention Guidance)

The DoIT IT Security Manual focuses on the minimum security requirements needed to adequately protect the confidentiality, integrity, and availability of Maryland Information Systems and State-owned data.

These security requirement responsibilities for State-owned data extend to all agency information while it is being processed, stored, or transmitted electronically.

Background – PII - State Security Requirements (cont.)

For PII data protection, the DoIT IT Security Manual, defines the following related key security requirements:

- PII Identification - Manual Section – Configuration Management, part CM-8, requires information systems components be inventoried, including components holding PII.
- PII Data Retention - Manual Section – Data Minimization and Retention directs agencies to collect, use, and retain only relevant PII necessary for the original purpose for which it was collected.
- PII Data Protection - Manual Section – Asset Management recommends using encryption technologies and/or other substantial mitigating controls (such as Data Loss Prevention, Network Security Event Monitoring, and strict database change monitoring).
  - Encryption is the strongest, and preferred, control, and is the defense of last resort for critical PII data.

Overview – PII Within State IT Systems

Stored sensitive PII information is very prevalent within the information systems of State and local government agencies audited by OLA, shown by the types of agencies listed below and their related functions:

- State Universities and Colleges
- Comptroller Taxation Agencies
- Professional Licensing Agencies
- Transportation Related Agencies
- Benefit Related Agencies (Department of Human Services, Maryland Department of Health – Medicaid, Department of Labor) and their related claims information systems
- Other Health Related Agencies
- Judicial / Courts Related Agencies
- Public Safety Agencies' Information Systems
- Local Education Agencies (School Systems)

Overview – State IT Systems & Volume of PII Records

Total PII records within State agencies IT systems is substantial. Later in this presentation, we determined that for issued OLA audit reports from FY 2014 to 2020 (to date), a total of approximately 37,900,000 PII records existed, which were not subject to having adequate PII data security controls.

Notably, it is plausible that one Maryland citizen's PII data (just name and Social Security Number) could be held within the IT Systems of multiple state agencies. For example, an individual's PII could potentially exist within most or all of the IT systems of the agencies listed on the preceding slide.

Background – PII - Data Security Risks

Sensitive PII stored on State agencies information systems presents the following potential data security risks which include:

- PII data identification not being performed
- Improper PII data retention
- Unsecured Stored PII Data - which can lead to:
  - Improper Disclosure / Data Breach
  - Exfiltration (with associated unplanned dollar costs)

Those risks can expose State agency maintained PII to identity-theft crimes, the impact of which could be costly.

- Financial Losses and remediation expenses
- Lost Confidence in State Information Systems
- Operational impact through the disruption of daily State agency operations

Background – PII - Data Security Risks

Financial cost of PII data breach

Annually, the Ponemon Institute, in conjunction with IBM, publishes a Report on the Costs of a Data Breach. This Institute is an independent research organization focused on data protection and information technologies. Their 2019 report (for 507 companies) noted that for US-based organizations:

- Average data breach size – 25,575 records
- Average total data breach cost - $8,200,000
- Cost per lost record - $242

The cost elements above include detection and escalation, notifications, response and lost business.

In addition to the immediate costs, data breaches have lifecycles (from occurrence to containment) and long tails (costs extending for years after an incident).

PII Data – General OLA Audit History

- On Sept 27, 2012, OLA issued a Performance Audit Report on the Department of Information Technology and Selected State Agencies on Information System Data Security.

- Finding 1 in the audit report disclosed that then current State law (the Maryland Personal Information Protection Act) regarding PII data protection did not apply to State agencies, and, that there was no applicable State law for the protection of PII by governmental units.

- The aforementioned OLA audit report, coupled with the efforts of the Commission on Maryland Cybersecurity Innovation and Excellence, led to the 2013 enactment of SB676 (Governmental Procedures – Security and Protection of Information), which established PII data protection requirements for units of State and local government (effective July 1, 2014).

PII Data – Individual OLA Audits

- During the period from fiscal year 2014 through November 2019, OLA issued 457 reports resulting from audits and reviews of State and local government units.
- 77 of these 457 audit reports (16.8%), involving 69 units of State and local government, identified 84 findings concerning the lack of adequate controls over the protection of PII.
- Across the above cited 77 audit reports, approximately 37.9 million records were identified as containing PII data elements (for example names and SSNs) where the lack of controls left the records susceptible to increased risk of improper disclosure.
- In response to these audit reports, the agencies generally agreed with our findings and recommendations. Notably, 12 of these 84 noted findings were repeats of audit findings cited in prior audit reports due to corrective actions not being implemented.

PII – Control Issues Commonly Identified in Audits

- **PII Data Protection** - PII data, mainly in a recorded at rest mode was stored in a plain text format, without being either encrypted, or with alternative substantial mitigating controls to safeguard the PII data from improper disclosure. This issue was cited in 49 of the 84 audit findings (33.1 million records susceptible to increased risk).
- **PII Data Access** – Restricted access to stored PII data did not always exist per the concept of least privilege. Certain audits identified instances where granted PII data access was unnecessary, because the access was either not needed or was excessive for the system users' job responsibilities. This issue was cited in 9 of the 84 audit findings.
- **PII Data Policies** - Agencies had not established adequate policies over the protection of PII or had relied on external service providers to process PII without ensuring the information was adequately safeguarded (such as by requiring independent security assessments). This issue was cited in 26 of the 84 audits findings.

PII Control Issues – Causes for Audit Findings

OLA believes the causes for unsecured PII within audited State and local agencies IT systems, include, but are not limited to, cases of:

- Agency management being unaware of the need to inventory and secure PII data;
- Unexpected PII records;
- Outside service provider contracts not including requirements for either independent security reviews (e.g., SOC 2 Type 2) and/or PII data encryption;
- Commercial off the shelf software that either lacked an encryption capability or the capability could not be implemented;
- Encryption usage causing system performance issues: and/or
- IT staff technical knowledge limitations.

Agencies have generally not cited a lack of budgetary resources as a cause for our PII findings.

Conclusions - State of Maryland – PII Data Protection

- Clearly understood State law PII data definitions exist
- Clear PII data security protection requirements have been established and defined
- The existence of PII data in State government IT systems is pervasive
- Agencies IT systems' PII data carries inherent security risks and State IT systems always have protection features available
- OLA audit history shows that PII data protection issues continue to be problematic. Between FYs 2014 and 2020, the count of reports containing PII-related findings, by FY, were:

2014 – 6	2015 – 16	2016 – 7	2017 – 11
2018 – 16	2019 – 12	2020 - 9	

- Some agencies are not establishing adequate control over PII, which requires increased, diligent, and focused efforts, with assistance provided by key control agencies, such as DoIT.

Recommendations - PII Data Protection

Adequate security protection over State IT information systems PII requires a twofold approach by control agencies and individual State agencies.

Control agencies, such as DoIT, the USM Office, and the Judiciary Administrative Office of the Courts, for agencies under their oversight, on an ongoing basis should advise and reinforce to those agencies:

- the prevalent existence of PII data;
- the significance of PII data, as per the State statutes;
- the financial risk to the State of Maryland arising from unsecured PII data;
- reiterate the necessary PII data protection controls (i.e., identification, encryption, and data access limitations);
- monitor agencies' progress in implementing PII data protection controls; and
- offer general and technical assistance, as needed, to individual agencies pursuing PII data protection.

Recommendations - PII Data Protection (cont.)

For adequate security protection over State IT information systems PII, individual agencies need to:

- implement either approved encryption methods to encrypt PII both at rest and when transmitted, or substantial mitigating controls (such as the use of Data Loss Prevention solutions) to ensure that confidentiality is protected;
- perform periodic reviews of system access to PII to ensure that access is assigned/restricted based on the concept of least privilege and is removed when such access is no longer required for legitimate business purposes; and
- establish agency specific policies and procedures for protecting PII when a third-party service organization is involved, including requiring that independent security assessments, such as SOC 2 Type 2 reviews, are performed, reported to the agency, and reviewed by the agency, with agency verification that any necessary correction actions are implemented.