Department of Legislative Services
Office of Legislative Audits

Department of Information Technology (DoIT)

and

Selected State Agencies

Information System Data Security

Report Dated September 27, 2012

Presentation to the Joint Audit Committee

Thomas J. Barnickel III, CPA
Timothy R. Brooks, CPA, CFE
Edward L. Shulder, CPA

October 16, 2012

Audit Overview

- DoIT was established July 1, 2008 by law with specified responsibilities which include:
  - Developing, maintaining, revising, and enforcing information technology (IT) policies, procedures, and standards for Executive Branch agencies.
  - Providing technical assistance, advice, and recommendations about IT matters to any State government unit.
- DoIT developed and issued an *Information Security Policy (Policy)* that sets the minimum standard requirements that agencies must meet to protect the confidentiality, integrity and availability of State-owned information. DoIT's practice has been to update the *Policy* on an annual basis.

Audit Overview (continued)

- DoIT has 119 positions organized into eight divisions with fiscal year 2011 expenditures totaling $55.8 million ($16.4 million for major information technology projects).

- The audit had two objectives:

  - To evaluate State law and DoIT's September 2010 *Policy* against industry information security best practices and federal and other states' practices.

  - To assess compliance with certain aspects of DoIT's *Policy* by selected State agencies with automated systems containing confidential information and to determine the extent of the agencies' implementation of recognized security best practices that were not addresses by DoIT requirements.

Audit Overview (continued)

- The State agencies reviewed for this audit were:
  - Comptroller of Maryland (Comptroller)
  - Department of Health and Mental Hygiene (DHMH)
  - Department of Public Safety and Correctional Services (DPSCS)
  - Department of Human Resources (DHR)
  - Department of Transportation – Motor Vehicles Administration (MVA)

- State agencies maintain significant volumes of personally identifiable information (PII), such as social security numbers, that relate to income taxes, medical assistance program claims histories, criminal backgrounds, public assistance, and driver's licenses. PII is often sought for identity-theft crimes.

Audit Overview (continued)

- External security risks have significantly increased due to states offering additional services online, and collecting, storing, and sharing information across public networks.

- Breaches of that information could harm citizens, businesses, and the State's public image and could result in significant expense to remediate the situation.

- Breaches to either obtain PII or disrupt government services could be attributable to parties external to the organization or to its own employees.

- Individual employee negligence is a significant threat to data security and contributed to 41% of the breaches reviewed in one study.

Audit Overview (continued)

- Performance audit results in brief:
  - We developed five recommendations for DoIT to improve the *Policy* requirements and guidance it provides to State agencies, including enforcement of its *Policy*.
  - We also developed seven recommendations applicable to all State agencies that could improve their data security practices to better protect the confidentiality, integrity, and availability of State-owned data, including PII.
- DoIT and the State agencies reviewed generally agreed with the recommendations.

Key Audit Issues

- State law governing protections for PII did not apply to State agencies. State law notification requirements about data breaches applicable to businesses were not addressed in DoIT *Policy*.
- Although State law assigns to DoIT the responsibility for enforcing information security, DoIT had not developed a process to monitor and enforce its *Information Security Policy* and instead delegated this responsibility to the individual agencies.
- Certain enhancements to DoIT *Policy* could be made, such as providing complete guidance to State agencies for handling and reporting computer security incidents.
- None of the five State agencies we examined had implemented all seven of the DoIT *Policy* requirements selected for review; all 5 agencies could improve their data security practices.

Protections for Personally Identifiable Information

- Current State law governing certain protections for PII did not apply to State agencies, nor were certain of these protections addressed in the DoIT *Policy. (Finding 1)*
- The Maryland Personal Information Protection Act requires business to protect PII and outlines the actions to be taken in the event of a breach, such as investigating if the breach resulted in the misuse of PII, and notification of affected individuals, credit reporting agencies, and the Office of the Attorney General.
- No State law or statewide policy existed that requires State agencies to be held to similar standards.
- 46 states have security breach notification laws involving personal information. 34 of these specifically include government as an entity subject to the laws' investigation and notification provisions that are similar to those applicable to Maryland businesses.

Information Security Policy Enforcement

- Although State law includes enforcement of information technology polices, procedures, and standards as one of DoIT's responsibilities, DoIT had not developed any formal mechanism to monitor and enforce its *Policy*. (Finding 2)

- For example, DoIT did not determine whether State agencies performed risk assessments, developed appropriate security protocols, conducted vulnerability assessments, or performed other actions called for by its *Policy* to protect confidential data maintained on agencies IT systems.

- We were advised that DoIT delegated the enforcement responsibilities to the individual agencies due to its lack of available resources for review and enforcement.

Handling and Reporting of Security Incidents

- The DoIT 2010 *Policy* did not provide complete guidance for handling and reporting computer security incidents. (Finding 3) Specifically it,
  - did not provide guidance for developing an incident response policy and plan, selecting an incident response team, and staffing and training the team, and
  - did not require agencies to report IT incidents to DoIT, until the 2012 *Policy* revision.
- Between June 2009 and June 2011, DoIT received only five IT incident reports from State agencies although agencies advised us that they had more incidents.
- Based on our regular audits, State agencies may not be aware of all security incidents. In 34 OLA audit reports issued from 7/2008 to 1/2012, we identified agency deficiencies in generating or reviewing security logs.

DoIT Guidance to Agencies

- DoIT had not provided complete or timely guidance to State agencies in other areas (Findings 3, 4 & 5) such as:
  - security for mobile devices
  - emerging technologies such as cloud computing
  - vulnerability scanning and penetration testing which can disclose system and software weaknesses and inadequate security awareness of individuals for remediation, and
  - data loss prevention software that can detect and restrict the unauthorized transmission or disclosure of confidential information.

Selected State Agency Security Practices

- None of the five agencies had implemented all seven of the DoIT *Policy* requirements selected for review:

Security Categorization of IT Systems (Finding 6)

- Only one agency (Comptroller) had determined and documented the security levels for all of its information systems as required by DoIT, which is integral for assessing the risks associated with data confidentiality, integrity, and availability.

- Three agencies (DHMH, DHR, MVA) had not assigned security categories for any of their systems.

- Another agency (DPSCS) assigned security categories only for certain of its systems.

Selected State Agency Security Practices (cont'd)

Agency Specific Information Security Policy
(Finding 7)

- Only 3 agencies (Comptroller, DHMH, MVA) had developed agency specific security policies that met DoIT requirements for their particular security environments, agency missions, and operational requirements.
- One agency's (DPSCS) policy did not address the specific aspects of its systems but merely copied DoIT policy without any guidance on how the agency implemented the related requirements.
- Another agency's (DHR) policy did not address security certification and accreditation for its systems.

Selected State Agency Security Practices (cont'd)

Risk Management Process (Finding 8)

- None of the 5 agencies had fully implemented a risk management process for all of its systems nor established a frequency for conducting reassessments.

- The risk management process identifies the risks, assesses the risk levels, and implements steps to mitigate risks to an acceptable level and continuously monitors the security state of each system.

Selected State Agency Security Practices (cont'd)

Security Awareness Program (Finding 9)

- All 5 agencies had developed security awareness programs for their employees with appropriate content for protecting systems and data security. However,
  - Three agencies (Comptroller, DHMH, DHR) did not ensure or document that employees received the required training.
  - One agency (MVA) had numerous employees who had never received the agency required security training.
  - Only one agency (DPSCS) had documented that initial and periodic retraining was provided to all employees as required.

Selected State Agency Security Practices (cont'd)

Confidential Information on Portable Devices (Finding 10)

- Two agencies (DHMH, DHR) had not taken adequate steps to protect confidential information stored on portable devices to ensure such information was protected from disclosure in the event the device was lost or stolen.

- The other three agencies (Comptroller, DPSCS, MVA) implemented procedures to encrypt confidential information on portable devices.

Inventory of Information Systems (Page 30)

- All 5 agencies maintained an adequate inventory of their IT systems and applications.

Selected State Agency Security Practices (cont'd)

Incident response Process (Page 35)

- All 5 agencies had developed a process for responding to potential information security incidents that met DoIT's *Policy* requirements at the time of the audit. (Although, as noted in Finding 3, DoIT needs to enhance policy guidance in this area.)

Use of Certain Information Security Best Practices

- Two agencies (Comptroller, DHR) had implemented data loss prevention tools to monitor email activity for certain patterns (such as social security numbers) and flag such activity for further review. (Finding 11)

- Three agencies routinely performed vulnerability scanning and two of these agencies also performed penetration testing . (Finding 12)

Conclusions

DoIT needs to:

- address the protection of PII in the custody of State agencies via legislation or policy, and the notification of affected individuals and other appropriate parties in the event of a breach.

- implement a process to monitor and enforce State agencies' compliance with its *Information Security Policy*.

- establish more thorough security incident response guidance in its *Policy*.

- enhance its security polices and guidance in other areas identified in the audit report, including emerging technologies.

Conclusions (continued)

State agencies need to ensure that they:

- comply with DoIT policies for evaluating and documenting the security categories for their systems and establish security measures commensurate with data sensitivity and risk.
- develop agency-specific information security policies that address DoIT's required components of an information security program.
- develop and implement a risk management process for all critical systems and periodically update or re-evaluate the risk assessments.
- provide security awareness training timely to all employees,
- ensure that confidential information on portable devices is encrypted, and that data loss prevention, vulnerability scanning and penetration testing tools are used as feasible.