

Performance Audit Report

Department of Information Technology and Selected State Agencies

Information System Data Security

Department of Information Technology Needs to Develop a Process to Monitor
and Enforce the Provisions of its *Information Security Policy*

State Agencies Should Comply With the Provisions of the *Information Security
Policy* to Help Ensure the Protection of Confidential Information

September 2012



OFFICE OF LEGISLATIVE AUDITS
DEPARTMENT OF LEGISLATIVE SERVICES
MARYLAND GENERAL ASSEMBLY

-
- This report and any related follow-up correspondence are available to the public through the Office of Legislative Audits at 301 West Preston Street, Room 1202, Baltimore, Maryland 21201. The Office may be contacted by telephone at 410-946-5900, 301-970-5900, or 1-877-486-9964.
 - Electronic copies of our audit reports can be viewed or downloaded from our website at <http://www.ola.state.md.us>.
 - Alternate formats may be requested through the Maryland Relay Service at 1-800-735-2258.
 - The Department of Legislative Services – Office of the Executive Director, 90 State Circle, Annapolis, Maryland 21401 can also assist you in obtaining copies of our reports and related correspondence. The Department may be contacted by telephone at 410-946-5400 or 301-970-5400.
-



DEPARTMENT OF LEGISLATIVE SERVICES
OFFICE OF LEGISLATIVE AUDITS
MARYLAND GENERAL ASSEMBLY

Karl S. Aro
Executive Director

September 27, 2012

Bruce A. Myers, CPA
Legislative Auditor

Senator James C. Rosapepe, Co-Chair, Joint Audit Committee
Delegate Guy J. Guzzone, Co-Chair, Joint Audit Committee
Members of Joint Audit Committee
Annapolis, Maryland

Ladies and Gentlemen:

We conducted a performance audit to assess State law and policies governing information security as compared to industry and government best practices and to determine compliance with certain aspects of the State information security policy by selected State agencies. The protection of information systems is necessary to ensure confidentiality, integrity, and availability of the information contained in those systems. A breach of confidential information, such as personal identifiable information (PII), could harm citizens and businesses of the State and could cause the State to incur significant expenses to remediate the situation. A number of information security breaches have occurred involving confidential data maintained by governments, including State governments.

Our audit disclosed that the Department of Information Technology (DoIT) had not developed a process to monitor and enforce the provisions of its *Information Security Policy*, although State law includes enforcement of information technology (IT) policies, procedures, and standards as one of DoIT's responsibilities. For example, DoIT had not established a formal mechanism to determine if agencies had developed appropriate security strategies to address the risks associated with their information systems and related data. Rather, according to DoIT's *Policy*, the responsibility for assessing compliance with the *Policy's* IT security requirements has been delegated to each State agency.

Our review of the security programs of five State agencies that maintain confidential data on information systems disclosed that all five agencies could improve their policies and practices. Specifically, none of the agencies had implemented all of the DoIT *Policy* requirements we selected for review. For example, we found that only one of the five agencies had determined and documented security levels for all of its information systems, which is integral

for assessing risks associated with data confidentiality, integrity and availability. None of the five agencies had fully implemented a risk management process.

Our audit also disclosed that, unlike many other states, current State law governing certain protections related to PII, such as social security numbers, did not apply to PII held by State government agencies. Furthermore, certain notification requirements involving data breaches established in the law for businesses were not addressed in DoIT's *Policy*. We also identified opportunities for DoIT to make enhancements to its *Policy* and related guidance to assist State agencies in meeting DoIT's requirements and implementing techniques to improve security practices.

An executive summary of our findings can be found on page 5, and our audit scope, objectives, and methodology are explained on page 9. The responses of DoIT and the five agencies selected for review during this audit are included as Appendix B to this report. We wish to acknowledge the cooperation extended to us by DoIT and those agencies during our audit.

Respectfully submitted,



Thomas J. Barnickel III, CPA
Acting Legislative Auditor

Table of Contents

Executive Summary	5
Audit Scope, Objectives, and Methodology	9
Background Information	13
Department of Information Technology (DoIT)	13
DoIT's <i>Information Security Policy</i>	13
Confidential Information	14
Information Security and Risks	15
Federal Government Information Security	17
Commission on Cyber Security Innovation and Excellence	18
Findings and Recommendations	21
Objective 1: State Law and DoIT Policies	21
Conclusion	
State Law Requirements	
Finding 1 – Current State Law Governing Certain Protections for Personal Identifiable Information Did Not Apply to State Agencies	21
Finding 2 – DoIT Did Not Have a Formal Process in Place to Enforce the Provisions of its <i>Information Security Policy</i>	23
DoIT <i>Information Security Policy</i>	
Finding 3 – DoIT Could Improve Guidance to Help Agencies Address Certain Security Issues	24
Finding 4 – DoIT Needs to Develop a More Responsive Process to Address Emerging Technologies and a Policy Regarding Mobile Devices	26
Finding 5 – DoIT Had Not Developed Recommended Practices for Implementing Data Loss Prevention Solutions	28
Objective 2: Selected State Agency Security Practices	29
Conclusion	
Background	
Compliance with DoIT Security Policy Requirements	
Inventory of Information Systems	
Finding 6 – State Agencies Often Did Not Document the Security Categorization of Information Systems	31
Finding 7 – Certain Agencies' Information Security Policies Were Not Agency Specific or Did Not Include All Required Components	32

Finding 8 – Risk Management Processes Were Not Fully Implemented	33
Finding 9 – Security Awareness Training Was Not Always Provided to Employees or Tracked	34
Incident Response Process	
Finding 10 – Data Contained on Portable Devices Was Not Always Properly Protected	35
Use of Certain Information Security Best Practices	
Finding 11 – State Agencies Were in Various Stages of Implementing Data Loss Prevention Tools and Techniques	36
Finding 12 – State Agencies Had Varied Practices in Implementing Vulnerability Scanning and Penetration Testing	37
Glossary	Appendix A
Agency Response	Appendix B

Executive Summary

Legislative Audit Report on the Department of Information Technology and Selected State Agencies Information System Data Security September 2012

We conducted a performance audit to assess State law and policies governing information security as compared to industry and government best practices and to determine compliance with certain aspects of the State information security policy by selected State agencies¹.

The Department of Information Technology (DoIT), established in July 2008, is responsible for overseeing the State's information technology (IT) function including developing, revising, and enforcing policies, procedures and standards related to IT. To assist in compliance with its mandated responsibilities, DoIT developed the *Information Security Policy (Policy)*. The *Policy* in existence during the audit was issued in September 2010. An updated version became effective in April 2012 (for report purposes, we refer to the September 2010 *Policy* as the 2010 *Policy* or just the *Policy*). The *Policy* outlines DoIT and agency information security responsibilities. In addition to the DoIT *Policy*, the federal government, as a result of the 2002 Federal Information Security Management Act, has developed a number of information security policies and guidance documents, some of which have been incorporated by reference into the DoIT policy.

Objective 1 – Evaluation of State law and DoIT's Information Security Policy

Unlike many other states, current State law governing certain protections for personal identifiable information (PII), such as social security numbers, did not apply to PII held by State government agencies. Furthermore, certain notification requirements involving data breaches established in State law for businesses were not addressed in the DoIT *Policy*.

Although State law assigns to DoIT the responsibility for enforcing information security, DoIT had delegated this responsibility to the individual agencies. Consequently, DoIT had not established a formal oversight process for ensuring that State agencies took appropriate actions to protect information

¹ Definitions/descriptions of commonly used technical terms contained in this report are contained in the Glossary, see Appendix A.

systems and data by complying with its *Policy*. We were advised that the delegation of its enforcement responsibilities was due to the lack of personnel resources. Nevertheless, in view of the findings identified in objective 2 of this audit report and the significant costs should a major security breach occur, additional oversight efforts are needed.

The 2010 *Information Security Policy* includes a number of appropriate practices and guidance for State agencies, but some enhancements could be made. For example, the *Policy* provided only limited guidance to agencies for handling and reporting computer security incidents (such as unauthorized access or denial of service attacks). Further, the 2010 *Policy* does not require State agencies to report incidents to DoIT or affected individuals, although the April 2012 revision does specify that agencies shall report incidents to DoIT. We found through a survey of State agencies that only five computer incidents were reported to DoIT for the period from June 2009 to June 2011 even though the agencies advised us that they had internally identified significantly more incidents than those reported to DoIT. The 2010 *Policy* and April 2012 revision also did not address information security concerns for mobile devices that can be used to store and process data (such as smart phones and tablet computers). Although some State agencies have used cloud computing services for a number of years, the *Policy* did not address the use of these services until the April 2012 revision.

Objective 2 – State Agency Compliance with DoIT Policy and Industry Best Practices

We reviewed certain agencies' security policies and practices for compliance with seven specific requirements of the DoIT *Policy* and found that the five State agencies selected for the review had implemented various components of an information security program. However, none of the agencies reviewed had implemented all program components required by DoIT. For example, we found that only one of the five agencies we reviewed had determined and documented security levels for its information systems, which is integral for assessing risks associated with data confidentiality, integrity and availability. We also found that the agencies did not fully implement risk management processes, which require an entity to identify security risks, assess those risks, and take steps to reduce those risks to acceptable levels. Two of the agencies had completed risk assessments for data centers housing agency information systems but none of the five agencies assessed and addressed risk for all of its individual information systems. State agencies also need to take steps to better protect data stored on portable devices such as laptops.

Two of the agencies that authorized the use of portable devices for the storage and access of PII (such as personal health data) did not adequately protect the data (such as through the use of full disk encryption).

Certain agencies reviewed had implemented industry best practices (security processes or techniques not specifically required by DoIT *Policy*) but additional steps could be taken. For example, while two agencies had implemented data loss prevention processes (such as scanning e-mails for release of potentially confidential data) in order to better protect agency information, the remaining three agencies had not instituted any such practice. Finally, we found that State agencies need to implement vulnerability scanning and determine the need for penetration testing. These processes are designed to help protect agency information by ensuring that information systems are protected against known vulnerabilities (scanning) and tested against outside attacks (penetration testing).

Audit Scope, Objectives, and Methodology

Scope

We conducted a performance audit to assess State law and policies governing information security as compared to industry and government best practices and to determine compliance with State information security policy by selected State agencies. The protection of information systems is necessary to ensure confidentiality, integrity, and availability of the information contained in those systems². We conducted this audit under the authority of the State Government Article, Section 2-1221 of the Annotated Code of Maryland and performed it in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Objectives

Our audit had two objectives:

1. To evaluate State law and the Department of Information Technology's (DoIT) September 2010 *Information Security Policy (Policy)* against industry information security best practices and federal and other states' practices.
2. To assess compliance with certain aspects of DoIT *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 addressed by DoIT requirements.

Methodology

To perform the audit, we reviewed a number of security related reports and publications applicable to both the public and private sectors, including those issued by information security firms. We also reviewed relevant information prepared by the National Conference of State Legislatures.

² Definitions/descriptions of commonly used technical terms contained in this report are contained in the Glossary, see Appendix A.

Objective 1

To accomplish this objective, we reviewed applicable State laws, as well as information security policies and procedures established by DoIT. We conducted research and reviewed information security laws applicable to the federal government and other states. We identified policies used by these entities in fulfilling the requirements of their respective laws. We evaluated the 2010 *Policy* (which was the most current policy available at the time of our audit work) against existing federal guidance. We also interviewed DoIT personnel responsible for information security policy development.

Objective 2

To determine which State agencies we would review for this objective, we surveyed approximately 100 State agencies in May 2011 to identify the scope of agency systems and agencies with information systems that contained private or sensitive data (that is, personal identifiable information – PII – as defined in the Glossary, Appendix A). Of the 58 responses we received, 49 indicated they maintained private or sensitive data as defined by DoIT *Policy* in their information systems. We judgmentally selected specific State agencies for review and testing based on the information contained in the surveys, and our determination of the existence of PII in information systems based on OLA's statutorily required audits of State agencies (performed once every three years). The following five agencies were selected for review and testing (the parentheses include examples of the types of confidential data each of the agencies maintains on its systems):

- Comptroller of Maryland – Comptroller – (income tax return information, bank account information, State corporate purchasing card data)
- Department of Health and Mental Hygiene – DHMH – (Medicaid recipient data, various disease and health care program data, vital records)
- Department of Public Safety and Correctional Services – DPSCS – (sex offender data, criminal and other offender based data)
- Department of Human Resources – DHR – (assistance program participant data including children in foster care, child support data including data on custodial parents, non-custodial parents and their children)
- Maryland Department of Transportation – Motor Vehicle Administration – MVA – (driver license files)

We obtained agency security program documents and evaluated specific security requirements based on the DoIT *Policy* (such as agency determination of security categories for systems and a formal risk management process).

The specific components evaluated are included in more detail later in this report (under Objective 2 Findings and Recommendations). We interviewed agency personnel responsible for information system security and evaluated agency policies and procedures, conducted tests of practices when practicable, and reviewed agency security assessments when available. Finally, we determined if the selected agencies implemented certain best practices (such as data loss prevention programs) not specifically required by the *Policy*.

Our audit did not include the evaluation of compliance with certain DoIT *Policy* requirements that are included in our statutorily required audits of State agencies (performed once every three years). This includes disaster recovery plans, network and system configuration, and user access and password controls. In addition, we did not assess security practices over paper records that may contain confidential information. Finally, our audit did not include any assessment of the University System of Maryland colleges and universities as these agencies are not subject to policies established by DoIT.

Fieldwork and Agency Response

We conducted our fieldwork from May 2011 to December 2011. DoIT's and the five agencies' responses to our findings and recommendations are included in Appendix B to our audit report. As prescribed in the State Government Article, Section 2-1224 of the Annotated Code of Maryland, we will advise the applicable state agencies regarding the results of our review of their responses.

Background Information³

Department of Information Technology

Chapter 9, Laws of Maryland 2008, effective July 1, 2008, established the Department of Information Technology (DoIT) as a principal unit of the Executive Branch and transferred the information technology and telecommunications functions of the Executive Branch from the Department of Budget and Management – Office of Information Technology to DoIT. For fiscal year 2011, DoIT's expenditures totaled \$55.8 million (including \$16.4 million for major information technology projects). DoIT is organized into eight divisions with a total staff of 119 budgeted positions. By law, DoIT's responsibilities include:

- developing, maintaining, revising, and enforcing information technology (IT) policies, procedures, and standards applicable to Executive Branch agencies, except for the University System of Maryland, and commissions of State government;
- providing technical assistance, advice, and recommendations concerning information technology matters to any unit of State government;
- reviewing the annual IT project plan for each unit of State government to make information and services available to the public over the internet; and
- developing and maintaining the Statewide Information Technology Master Plan.

DoIT's *Information Security Policy*

In accordance with its legal mandate to set policy and provide guidance and oversight for the security of IT systems, DoIT developed and issued an *Information Security Policy (Policy)*. The *Policy* describes the set of minimum standard requirements that Executive Branch agencies must meet in order to protect the confidentiality, integrity, and availability of State-owned information. The initial version was issued in September 2009, and the revised version that was in effect at the time of our audit was issued in

³ Definitions/descriptions of commonly used technical terms contained in this report are contained in the Glossary, see Appendix A.

September 2010. In addition, DoIT's most recent *Policy* revision was released in October 2011 with an effective date of April 2012. It has been DoIT's practice to update the policy at least on an annual basis.

The *Policy* includes ten sections and outlines DoIT and agency responsibilities, and describes the components of an agency IT security program. DoIT requires a minimum of seven components for an agency IT security program. These components are:

- IT Security Policy
- Risk Management Process
- Systems Development Life Cycle Methodology
- IT Security Certification and Accreditation
- IT Disaster Recovery Plan
- Security Awareness
- IT Incident Process

Additionally, the *Policy* provides minimum requirements for certain areas such as asset management (such as having an inventory of assets), physical security (such as access to data centers and IT equipment), network security (such as monitoring agency networks), and user access control (such as ensuring that only authorized users have been assigned system rights to access the information).

Confidential Information

DoIT's *Policy* defines confidential information as non-public information that if disclosed would result in a highly negative impact to the State of Maryland, its employees or citizens, and may include information or records deemed as private, privileged, or sensitive. The *Policy* also considers personal identifiable information (PII) as a form of confidential information.

According to the Commercial Law Article, Section 14-3501 of the Annotated Code of Maryland (part of the Maryland Personal Information Protection Act), personal information is an individual's first name or initial and last name in combination with any one or more of the following information:

- Social Security number;
- driver's license number;

- financial account number, including a credit card number or debit card number, that in combination with any required security code, access code, or password, would permit access to an individual's financial account; or
- individual taxpayer identification number

Personal information (commonly referred to as PII), does not include personal information when that information is encrypted, redacted, or otherwise protected by another method that renders the information unreadable or unusable.

Information Security and Risks

State agencies maintain a comprehensive set of citizens' PII as needed to facilitate agency operations. For instance, the State has information related to medical assistance program claims histories, income taxes, public assistance, criminal backgrounds, and driver's licenses. This type of information often is sought by those who wish to commit certain crimes (for example, identity theft and disruption of government services). Citizens entrust their information to the State; a breach of that information could harm citizens, businesses, and the State's public image and could cause the State to incur otherwise unneeded expense to remediate the situation.

Data Breaches in the United States

The Privacy Rights Clearinghouse has been tracking data breaches since 2005 and counts the number of records leaked that contain information useful to identity thieves (such as social security numbers)⁴. The Clearinghouse tracked 535 breaches reported in the United States in 2011 involving 30.4 million sensitive records. One of the most significant data breaches identified for 2011 involved the compromise of data on 3.5 million individuals held by the State of Texas. The breach occurred when this data was left unencrypted on publicly accessible servers. Texas government officials attributed the breach to numerous failures to follow security procedures.⁵

⁴ The Privacy Rights Clearinghouse is a nonprofit consumer organization established to raise consumers' awareness of how technology affects personal privacy, advocate for consumer privacy rights and provide practical tips on privacy protection.

⁵ Privacy Rights Clearinghouse, Data Breaches: A Year in Review, January 19, 2012.

In April 2012, Utah IT officials reported that health and Medicaid data for nearly 800,000 residents – including 280,000 Social Security numbers – had been stolen from a poorly secured server operated by the state's Department of Technology Services. In June of 2012, it was announced that Alaska's Medicaid office, which had a breach of approximately 2,000 patient records in 2009, will pay \$1.7 million to the U.S. Department of Health and Human Services (HHS) to settle possible violations of a federal law (HIPPA) that protects patient privacy. The Alaska agency had found that an employee's hard drive that may have contained protected health records of Medicaid beneficiaries had been stolen.

Other Security Studies and Surveys

A study of the cost of data breaches in the United States by the Ponemon Institute and Symantec stated that the average cost to an organization of a data breach in 2010 was \$7.2 million, up 7 percent from 2009⁶. The study also noted that total breach costs have grown each year since 2006. The average cost per compromised record in 2010 was \$214, up 5 percent from 2009. The study found that individual negligence continued to be the most common threat to data security and contributed to 41 percent of the breaches reviewed⁷. The study suggested that this may indicate that ensuring employee compliance remains an ongoing challenge.

A 2010 study by Deloitte and the National Association of State Chief Information Officers (NASCIO) confirmed that large amounts of PII that states maintain may be at risk, and securing PII is a daunting task⁸. The study commented on the lack of funding, resources, and tools available to state governments when compared to the private sector⁹. The study also stated that one-fifth of the reported security breaches in 2009 occurred in the state and local government sectors, based on their review of data loss notification websites¹⁰. It further reported that only 13 percent of the surveyed states (49 states responded to the survey) indicated that they had established procedures to measure the effectiveness of their information security. Meanwhile 27 percent of the states had little to no measurement of effectiveness¹¹.

⁶ Ponemon Institute, LLC and Symantec, 2010 Annual Study: U.S. Cost of a Data Breach, March 2011, page 6.

⁷ Ibid, page 7.

⁸ Deloitte and the National Association of State Chief Information Officers, State Governments at Risk: A Call to Secure Citizen Data and Inspire Public Trust, 2010, page 3.

⁹ Ibid, page 5.

¹⁰ Ibid, page 16.

¹¹ Ibid, page 11.

The Deloitte/NASCIO study also indicated that states lacked confidence in their ability to prevent internal threats when compared to external threats. Internal threats include an employee with authorized access who can distribute information to those outside of the organization or a disgruntled employee who intentionally causes service disruptions. External threats include someone from the general public who obtains information from the organization or disrupts the organization's operations or services by gaining unauthorized access to the organization's network or system. Furthermore, the study indicated that external security risks had significantly increased over the years due to states offering additional services online, and collecting, storing, and sharing information across public networks¹².

Furthermore, risks are changing with the adoption of new technologies. The 2010 Global Information Security Survey by Ernst and Young noted that 60 percent of survey respondents perceived an increase in the level of risk due to emerging technologies such as, social networking, cloud computing, and personal devices.¹³ When asked what they would do to address these new risks, 39 percent of the respondents said they would adjust policies, 38 percent said they would increase security awareness activities and 29 percent were implementing encryption techniques, among other controls.¹⁴

Federal Government Information Security

In 2002, the United States Congress passed the Federal Information Security Management Act (FISMA). The purposes of FISMA include a) to provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets; b) to develop and maintain minimum controls required to protect federal information and information systems; and, c) to provide for a mechanism for improved oversight of federal agency information security programs. Standards and guidance related to FISMA are issued by the National Institute of Standards and Technology (NIST) after approval by the Secretary of the U.S. Department of Commerce. To assist federal agencies in implementing information security, NIST issued Federal Information Processing Standard Publication 199 (FIPS Publication 199), FIPS Publication 200, and Special Publication 800-53.

¹² Ibid, page 19-20.

¹³ Borderless Security: Ernst and Young's 2010 Global Information Security Survey, page 4.

¹⁴ Ibid, page 7.

FIPS Publication 199 addresses standards for security categorization of federal information and information systems. These standards provide a common framework and understanding for expressing security that promotes effective management and oversight of information security programs. The standard requires categorization based on the consideration of three security objectives: confidentiality, integrity, and availability. Each of these objectives must be evaluated for potential impact (low, moderate, high) on organizations or individuals should there be a breach of security (that is, loss of confidentiality, integrity, or availability). FIPS Publication 199 describes the loss of confidentiality as the unauthorized disclosure of information, the loss of integrity as the unauthorized modification or destruction of information, and the loss of availability as the disruption of access to or use of information or an information system.

FIPS Publication 200 addresses minimum security requirements for federal information and federal information systems. This standard outlines 17 security-related areas (such as access control, incident response, and system and information integrity). The extent to which each area should be secured depends on the categorization of the information or information system as identified through the implementation of FIPS Publication 199.

Special Publication SP 800-53 addresses required security for each categorization (low, moderate, high). This publication provides federal agencies with guidelines for selecting and specifying security controls for information systems to meet the requirements of FIPS Publication 200.

Due to a lack of other authoritative guidance (such as standards promulgated by other state information security professionals) and the State's reference to NIST documents in its policy, we used these Publications as criteria for evaluating certain aspects of State agencies' information security practices.

Commission on Cyber Security Innovation and Excellence

Chapter 251, Laws of Maryland 2011, established the Maryland Commission on Cyber Security Innovation and Excellence. The Commission's purpose is to provide a road map for making the State the epicenter of cyber security innovation and excellence. The law set the requirements of the Commission (such as a review of State and federal cyber security laws, and policies, standards and best practices for ensuring the security of computer systems and networks used by State government and educational agencies). The law

further required the Commission to issue an interim report by January 1, 2012 of its findings and recommendations, including recommended legislation with a final report to be issued by September 1, 2014.

We reviewed the interim report issued by the Commission and noted that while the report contained a number of areas that will warrant further consideration by the Commission (including developing a template for state agencies to enact a proactive rapid response to cyber attacks and educating the public about the importance of cyber security), it did not contain specific recommendations. As a result, the report did not impact the findings or recommendations contained in this report.

Findings and Recommendations

Objective 1

State Law and Department of Information Technology (DoIT) Policies

Conclusion

We evaluated current State law and the Department of Information Technology's (DoIT) September 2010 *Information Security Policy (Policy)*. Our audit found that current State law that mandates certain processes and actions to protect personal identifiable information (PII) contained in information systems of businesses does not apply to State agencies and, as a result, did not mandate certain significant protective actions for data held by State agencies. Our audit also disclosed that DoIT had not developed a process to monitor and enforce provisions of its Policy, although State law includes enforcement of information technology policies, procedures, and standards as one of DoIT's responsibilities. We also found that while DoIT's *Policy* addressed a number of critical information security areas, the *Policy* should be enhanced. For example, the *Policy* provided only limited guidance to agencies regarding how to handle and report computer security incidents (such as unauthorized access or denial of service attacks). Furthermore, although the *Policy* required agencies to implement security monitoring, it did not provide any additional guidance on how to accomplish this. We also found that DoIT needs to ensure that it addresses security concerns for emerging technologies in a timely manner. Further, the *Policy* did not generally address the security implications of certain mobile devices that can be used to store and process information (such as smart phones and tablets).

Findings

State Law Requirements

Finding 1

Current State law governing certain protections for PII did not apply to State agencies and certain requirements established in State law also were not addressed in the DoIT *Policy*.

Analysis

Existing State law applicable to certain protections for PII does not apply to State agencies. In this regard, while provisions of State law prohibit State agencies from publicly posting personal information on an internet website, other protections required of businesses for such information are not required by law for State agencies. Specifically, the Commercial Law Article, Title 14, Subtitle 35 (Maryland Personal Information Protection Act) of the Annotated Code of Maryland, requires businesses to implement and maintain reasonable security procedures and practices to protect PII and outlines the actions to be taken in the event a business suffers a breach of security of a system (such as investigating if the breach resulted in the misuse of PII and notification of affected individuals, credit reporting agencies, as well as the Office of the Attorney General). However, this law does not include State agencies in the definition of a business subject to its provisions and there was no similar State law that would apply to State agencies.

Furthermore, no statewide policy existed that requires a State agency be held to similar standards to those established for businesses in this State law. The 2010 DoIT *Policy* defines breaches and encourages State agencies to report such breaches to DoIT. Although the April 2012 *Policy* revision states that agencies shall report breaches to DoIT, it does not require notification to any other party. DoIT advised us that they would consider modifying the *Policy* to include the provisions of State law regarding reporting, investigation, and notification.

According to the National Conference of State Legislatures (NCSL)¹⁵, as of October 2010, 46 states have security breach notification laws involving personal information. Our review of these laws disclosed that 34 (or 74 percent) specifically include government as an entity subject to the laws' investigation and notification provisions in a manner similar to what current State law requires for Maryland businesses. Generally, these laws define PII in a manner similar to Maryland.

Given the widespread adoption of laws by other states and the importance of securing PII and appropriately responding to breaches, we believe that there should be provisions in State law that address the protection of PII by State government entities.

¹⁵ NCSL is a bipartisan organization that serves the legislators and staffs of the nation's states, commonwealths and territories. NCSL provides research, technical assistance and opportunities for policymakers to exchange ideas on the most pressing state issues.

Recommendation 1

We recommend that DoIT

- a. propose legislation to address the protection of PII in the custody of State government agencies; and
- b. until such legislation is enacted, develop and implement a security breach notification policy containing requirements related to investigating system security breaches and notifying affected individuals and other parties as appropriate.

Finding 2

DoIT did not have a formal process in place to monitor and enforce the provisions of its *Information Security Policy*.

Analysis

Although State law includes enforcement of information technology policies, procedures, and standards as one of DoIT's responsibilities, DoIT had not developed any formal mechanism designed to monitor and enforce the provisions of its *Policy*. Specifically, DoIT did not ensure that State agencies had established comprehensive security programs in conformance with the *Policy* and monitored the effectiveness of their security programs. For example, DoIT had no formal mechanism in place to determine whether State agencies performed risk assessments, developed appropriate security protocols, conducted vulnerability assessments, or performed other actions specifically designed to protect confidential data on the State's information systems. Rather, according to DoIT's *Policy*, determining compliance with IT security requirements has been delegated to each State agency. We were advised that DoIT delegated this responsibility due to its lack of available resources for review and enforcement. DoIT currently has assigned four employees to address information security; however, these employees were primarily responsible for other aspects of computer security (such as granting and removing user access to the State's financial management information system and maintaining information security over systems used by DoIT and the Department of Budget and Management).

As a result, there was a lack of assurance that State agencies were complying with the provisions of the *Policy*. Given our audit findings at the agency level (see Objective 2) and the significant costs to an entity should a major security breach occur (as noted in the Background), efforts should be made to enhance oversight of State agencies subject to its *Policy*.

Although we did not conduct a comprehensive review of all other states with an oversight agency to determine legal authority to enforce computer security program requirements, our review of several other states with a department similar to DoIT and similar legal requirements disclosed that certain of the states had developed programs that facilitated more oversight of their state agencies' information security. For example, the Colorado Office of Information Technology – Office of Cyber Security has the responsibility for reviewing agency security plans, directing information security audits and assessments in public agencies to ensure program compliance, and reviewing agency information security plans on an annual basis. Furthermore, the Federal Department of Homeland Security (DHS) had instituted a process designed to annually review and follow up on federal agencies' information security programs (primarily through the use of agency self-assessments provided to DHS). With the adoption of the 2012 *Policy*, DoIT made certain self-assessment tools available for use by State agencies; however, the results of any self-assessments performed are not required to be submitted to DoIT.

Recommendation 2

We recommend that DoIT implement a process to monitor and enforce agency compliance with the *Policy*. For example, DoIT could consider requiring the use of an agency self-assessment tool as a means to help it ensure that State agencies have established comprehensive security programs and conduct ongoing monitoring of security effectiveness. Results of the self-assessments could be submitted to and used by DoIT to assist in monitoring and enforcing agency compliance with the *Policy*.

DoIT Information Security Policy

Background

As previously noted, DoIT has developed and issued an *Information Security Policy (Policy)* that sets the minimum standard requirements that agencies must meet in order to protect the confidentiality, integrity, and availability of State-owned information. To assist agencies in meeting the requirements of the *Policy*, DoIT has developed certain guidance material for agencies' use. DoIT also refers agencies to guidance developed by the federal government such as the National Institute of Standards and Technology (NIST).

Finding 3

DoIT could improve guidance to help agencies address certain security issues.

Analysis

While DoIT's *Policy* included information security concepts, DoIT did not include specific instructions or guidance regarding agency implementation of certain of these concepts. In this regard, DoIT's *Policy* referred to certain standards or guidelines published by NIST (for example, FIPS Publications 199 and 200), but often did not provide additional information or guidance to be used for implementation (such as by referring State agencies to other NIST publications). Specifically, we noted the following conditions:

- The 2010 *Policy* did not provide complete guidance to State agencies for handling and reporting computer security incidents. While the *Policy* defined what constitutes a computer incident (such as unauthorized access or a denial of service) and discussed the information technology incident response process, it did not provide specific guidance regarding how agencies should implement this process. Specifically, the *Policy* does not include (nor incorporate by reference) certain guidance that is included in NIST Special Publication 800-61. This publication states that agency incident response capability should include creating an incident response policy and plan, developing procedures for performing incident handling and reporting, selecting an incident response team structure, and staffing and training the team (among other requirements). In addition, all federal civilian agencies must report all incidents to a centralized entity and internally document corrective actions and related impacts. Until the April 2012 *Policy* revision, DoIT did not require agencies to report IT incidents to DoIT.

Furthermore, certain State agencies that are required to comply with incident reporting security requirements of other oversight agencies (federal government agencies) may not achieve such compliance despite having complied with the DoIT policy. In this regard, one agency provided us with a security report prepared by its federal oversight entity which stated that the agency had not adequately developed and implemented an incident response policy and related procedures as required by the oversight entity. Although we found that the tested agency's incident response policy complied with DoIT requirements, we note that the oversight entity's requirements are more detailed than those currently specified by DoIT.

Between June 2009 and June 2011, DoIT received only five IT incident reports from State agencies. In responding to our survey, agencies reported that they had internally identified significantly more incidents than those reported to DoIT. For example, three agencies reported that they had 10 more security incidents related to malicious code (such as malware) over the same two-year period. We were advised by the agencies that very few of the incidents required invoking their formal incident response process. New requirements that were established in DoIT's April 2012 *Policy* should improve the incident notification process within State government.

- The 2010 *Policy* requires agencies, at a minimum, to implement appropriate levels of security monitoring (such as penetration testing or vulnerability scanning) but the *Policy* did not provide guidance regarding how to perform such monitoring or what methods agencies should use. In addition, the April 2012 *Policy* revision no longer specifically refers to penetration testing as a method agencies could use to assist in securing its systems but still requires that agencies conduct security assessments. Further, the *Policy* did not refer to NIST guidance in this area. Specifically, NIST provides significant guidance on the use of penetration testing and vulnerability scanning in SP 800-115 (Technical Guide to Information Security Testing and Assessment).

Recommendation 3

We recommend that DoIT review the comprehensiveness of its existing *Policy* guidance pertaining to the information security concepts and provide additional instruction or guidance as necessary to agencies for implementing components of agency security programs.

Finding 4

DoIT needs to develop a more responsive process to address emerging technologies as well as a policy regarding the security requirements for mobile devices.

Analysis

DoIT needs to develop a more responsive process to address emerging technologies. While DoIT issues periodic updates to the *Policy* and meets with agency information security officers to discuss security and other information technology issues, DoIT did not always promptly address significant changes in technology impacting information security. Specifically, certain State agencies (such as the Department of Human Resources and Department of Health and Mental Hygiene – Mental Health Administration) have used cloud

computing services for a number of years; however, the September 2010 *Policy* does not address agency use and related security provisions associated with these services. The Cloud Security Alliance, a not-for-profit organization with a mission to promote the use of best practices for providing security assurance within cloud computing, issued *Security Guidance for Critical Areas of Focus in Cloud Computing*, dated April 2009, to address security best practices for cloud computing. The *Policy* revision effective April 2012 does contain sufficient guidance related to cloud computing.

We also found that DoIT had not developed comprehensive policies designed to guide agencies in providing security over mobile devices (such as smart phones and tablet computers). While the *Policy* includes a requirement that agencies approve the use of portable devices for storage of confidential information and the use of specified encryption technology¹⁶, it does not address a number of other potential security issues or requirements as related to mobile devices.

DoIT management advised us that it developed an internal policy regarding mobile device security. This policy, as currently written, applies only to DoIT issued mobile devices and not to other State agencies. We reviewed the internal DoIT policy and found that it incorporated a number of requirements that we also found in other states' policies on mobile devices including:

- The device must contain a password or pin to be accessed;
- Data on the device must be able to be wiped (removed) remotely;
- Operating systems and software must be up-to-date with the latest patches and security patches;
- The device must use anti-virus software;
- Third party applications must be disabled if there is no use for them; and
- Devices must be controlled and managed by a central authority.

While our review of the five State agencies in Objective 2 disclosed that the agencies generally did not currently use portable devices to transact official State business other than for e-mail, agencies did often allow the storage of PII (such as taxpayer and personal health data) on portable devices.

¹⁶ Encryption standards are referenced in NIST publication FIPS 140-2 (*Standards for Security Requirements for Cryptographic Modules*). NIST maintains a list of products that are certified to meet this encryption standard on its website.

Recommendation 4

We recommend that DoIT

- a. develop a process to more timely address the security implications of emerging technologies, and
- b. develop and issue a comprehensive statewide policy regarding minimum security requirements for mobile devices.

Finding 5

DoIT had not developed recommended practices for implementing data loss prevention solutions.

Analysis

DoIT had not developed recommended practices for State agencies to address data loss prevention (DLP) solutions. DLP is the process by which unauthorized transmission or disclosure of confidential information is detected and prevented, usually through the use of software that can discover, monitor, and restrict transmission of such information. According to a report issued by an information security company, one benefit of a DLP program is to prevent the accidental or malicious loss of data by an insider (an internal threat), for example, an employee¹⁷. The report also stated that a DLP program could reduce the cost of a data loss investigation if one was to occur, and would help with early detection or mitigation of such a loss¹⁸. Another report on data breaches occurring in 2010 found that 17 percent of the 761 breaches investigated in 2010 were caused by an internal threat¹⁹.

Certain steps required of a DLP program are included in the 2010 DoIT *Policy*. These steps include performing a risk assessment to determine the data maintained and the vulnerabilities associated with it, classifying the data based on its value and sensitivity, and training and awareness of inappropriate or harmful activities when handling sensitive information. However, the *Policy* does not address the need for a product that is used to prevent an unauthorized transmission of data an agency needs to protect.

Recommendation 5

We recommend that DoIT

- a. develop policy and guidance regarding the implementation of a data loss prevention strategy; and
- b. assist State agencies in researching, obtaining, and implementing data loss prevention tools.

¹⁷ Powell Hamilton, Foundstone Professional Services, Data Loss Prevention Program – Safeguarding Intellectual Property, page 7.

¹⁸ Ibid, page 7.

¹⁹ Wade Baker et. al., 2011 Data Breach Investigation Report, page 2.

Objective 2

Selected State Agency Security Practices

Conclusion

We reviewed five selected State agencies to determine the status of agency implementation of certain requirements of the DoIT *Policy* as well as adoption of certain industry best practices (not currently required by the *Policy*). We found that all five agencies had implemented various requirements of the *Policy*. However, none of the agencies had implemented all of the tested requirements and all of the agencies could improve their data security practices. For example, the agencies reviewed generally had not determined security categories for all information systems or implemented risk management practices as required by the *Policy*. State agencies also need to take steps to better protect data stored on portable devices.

Although not required by DoIT policies, some agencies have taken action to implement certain industry best practices such as data loss prevention programs and vulnerability scanning, but others have not initiated these practices.

Background

DoIT developed and issued its *Information Security Policy* in accordance with its legal mandate to set policy and provide guidance and oversight for the security of IT systems. The *Policy* describes the set of minimum standard requirements that Executive Branch agencies must meet in order to protect the confidentiality, integrity, and availability of State-owned information. In order to determine State agency compliance with DoIT's *Policy*, we selected for review five agencies with information systems containing confidential data. The following agencies were reviewed:

- Comptroller of Maryland – Comptroller
- Department of Health and Mental Hygiene – DHMH
- Department of Public Safety and Correctional Services – DPSCS
- Department of Human Resources – DHR
- Maryland Department of Transportation– Motor Vehicle Administration – MVA

We reviewed these agencies' policies and practices for compliance with certain elements of the 2010 *Policy* that would help secure information systems and related data. (Similar requirements are included in DoIT's April 2012 *Policy*.) Specifically, we determined the agencies' practices for complying with the following requirements of DoIT's *Policy*:

Asset management

- Inventory of information systems existed (Section 3.0 of the DoIT *Policy*)
- Security category determined for all identified information systems (Section 3.2)

Security Program

- Agency specific information system security policy existed (to include the components noted on page 14 of this report) (Section 4.0)
- Risk management process implemented (including risk assessments) (Section 4.1)
- Security awareness program implemented (Section 4.5)
- Incident response process established (Section 4.6)

Network Security

- Confidential data protection implemented for portable devices (Section 7.6)

In addition, we inquired as to whether these agencies implemented other industry best practices to help secure information systems such as DLP programs and vulnerability scanning and penetration testing.

Findings

Compliance with DoIT Security Policy Requirements

Inventory of Information Systems

The DoIT *Policy* requires agencies to maintain an inventory of its information systems and/or related applications. Inventories help ensure that effective asset protection takes place. Agencies need to be able to identify their assets and the relative values and importance of these assets to provide levels of protection commensurate with the value and importance of the assets. These assets include data and data files and the software (such as applications) used to process the data. To determine compliance, we asked each agency to provide a listing of all information system assets in use by the agency. We found that each agency substantially complied with this requirement by maintaining lists of these information system assets, which we determined were reasonably complete.

Security Categorization of Information Systems

Finding 6

State agencies often did not document the security categorization of their information systems.

Analysis

State agencies often did not document the security categorization of their information systems. The DoIT *Policy* on security categorization states that categorizing security applies to all State information systems and that agencies shall use FIPS Publication 199 which contains standards for categorizing information and information systems. Security category levels provide a framework that promotes effective management and oversight of information security programs and helps agencies determine the level of effort required to develop controls and address risks associated with information systems. Security categories are based on the potential impact on an organization should certain events occur which jeopardize the information and information systems needed by the organization. Security categories are to be used in conjunction with vulnerability and threat information in assessing the risk to an organization. Determining the security category of an information system requires the agency to consider the sensitivity of information that resides on the system and addresses the three security objectives (confidentiality, integrity and availability) for information and information systems. These security objectives are defined in more detail in the Glossary, Appendix A.

Our review disclosed that only one of the five agencies reviewed (Comptroller) had assigned security levels to all of its information systems. Another agency (DPSCS) assigned security categories but only for certain information systems. The remaining three agencies (DHMH, DHR, and MVA) did not assign security categories to any of their information systems.

Regarding the health and Medicaid data breach that occurred in Utah as mentioned earlier in this report, according to the former Utah CIO the best solution is better data classification. In a publicized interview dealing with the security breach, he explained that instead of trying to provide high-level protection for all information collected and used by agencies, governments need to get better at sorting data into categories based on its sensitivity and importance. He further opined that once those categories are established, they can be matched to the right security measures-highly sensitive records get the best, most expensive safeguards; less sensitive records receive less

attention²⁰. Furthermore, similar conclusions were reached by the U.S. Department of Health and Human Services (HHS) about the previously mentioned Medicaid data breach in Alaska. HHS concluded that the Alaska Medicaid office did not have sufficient policies and procedures to protect patient information. For example, the state health department had not completed a risk analysis for patient data.

Recommendation 6

We recommend that State agencies comply with DoIT *Policy* by evaluating and documenting security categories for all of their information systems and establish security measures commensurate with data sensitivity and risk.

Agency Specific Information Security Policy

Finding 7

Certain agencies' information security policies were not agency specific or did not include all required components.

Analysis

Agency security policies did not always meet the requirements of the DoIT *Policy*. According to the DoIT *Policy*, agency information security policies should address the fundamentals of agency information security governance (such as roles and responsibilities and rules of behavior). Agencies should develop policies to accommodate the information security environment and agency mission and operational requirements.

We found that three agencies (Comptroller, DHMH and MVA) met the criteria established by DoIT. That is, these agencies developed an adequate agency specific information security policy. However, one agency's (DHR) security policy did not address security certification and accreditation, one of the required seven components of an information security program. Detailed definitions of security certification and accreditation are provided in the Glossary, Appendix A. The remaining agency's (DPSCS) information security policy did not address specific aspects of the agency's information systems or operations and generally copied the information included in the DoIT *Policy* without any guidance on how the agency has implemented the related requirements. For example, the DPSCS Policy repeated the DoIT language for system certification and accreditation without any additional information on the process DPSCS uses to address the requirements. In addition, there was no evidence that system certification and accreditation had been performed.

²⁰ Steve Towns, "Lessons From a Breach," *Governing* magazine (July 2012), page 66.

Recommendation 7

We recommend that State agencies develop an agency-specific information security policy that addresses the required components of an overall information security program established by the DoIT *Policy*.

Risk Management Process

Finding 8

Risk management processes were not fully implemented.

None of the five state agencies selected for review had fully implemented a risk management process. Risk management refers to the process of identifying risk, assessing risk levels, and taking steps to reduce risk to an acceptable level. DoIT *Policy* and Federal guidance states that risk assessment is the first process in risk management (the other processes being risk mitigation and evaluation) and should be used to determine the extent of the potential threat and risk associated with an IT system.

However, we found that none of the five agencies had consistently completed risk assessments for all information systems (that is, each agency had performed certain risk assessments but not for all systems). For example, two agencies (Comptroller and DHR) completed risk assessments for data centers that housed agency information systems. But, in both instances, the risk assessments did not address the unique risks associated with the individual information systems (which may differ from the data center risks). Two of the agencies (Comptroller and DPSCS) advised us that they did not prepare risk assessments for certain systems due to the age of the systems. However, the relevant factor in assessing risk is the nature of the data (for example, does it contain PII or other confidential information), not a system's age.

NIST SP 800-30 (*Risk Management Guide for Information Technology Systems*) defines an information system as either a general support system (such as a mainframe computer or local area network) or a major application on such a system that satisfies a specific set of user requirements and details the steps an entity should follow to assess and mitigate risk for all information systems. SP 800-30 is incorporated by reference in the DoIT *Policy*.

Our audit also found that agency policies generally did not specify how often or under what circumstances the agency should complete or update risk assessments. NIST guidance states that good security practices include repeating the risk assessment process at least every three years.

Recommendation 8

We recommend that State agencies

- a. develop and document a risk management process including risk assessments that apply to all critical systems,
- b. specify how frequently risk assessments should be re-evaluated,
- c. perform risk assessments for all critical systems currently in use, and
- d. periodically update or re-evaluate the risk assessments.

Security Awareness Program

Finding 9

Security awareness training was not always provided to employees or tracked.

Analysis

While the agencies tested generally developed security awareness programs for their employees that included appropriate content, we found that certain agencies did not ensure that employees received training on such awareness or did not document such training. DoIT's *Policy* requires agencies to develop and implement a security awareness program that includes promoting awareness (such as appropriate Internet and e-mail use and how to handle confidential information) through formal instruction, web-based instruction, and various other methods. As noted earlier in this report, individual negligence is the most common threat to data security and ensuring employee compliance is an ongoing challenge.

Although one agency tested generally provided and documented the training provided (DPSCS), we found that three agencies (DHR, DHMH, and the Comptroller) did not adequately ensure or document that employees received required training. For example, at one agency (DHR), although training staff tracked locations it visited, it did not track actual employee attendance at these locations and, as a result, had no record indicating which employees had received the training.

For another agency (MVA), we found that new employees often did not attend training to promote security awareness as required by agency policy (that is, training was to be completed within 60 days of employment). According to the agency's automated training records, for the 69 new employees who started employment between May 1 and October 7, 2011, only 13 employees had completed the required training as of December 7, 2011. Many of these employees were in positions that provided access to confidential data maintained on information systems.

Recommendation 9

We recommend that agencies provide timely security awareness training to all employees and document employee attendance at the training.

Incident Response Process

Our review of the five agencies disclosed that all five agencies had developed a process for responding to potential information security incidents. Specifically, each agency's security policy included specific steps or actions to be taken in the event of a security incident as required by DoIT *Policy*.

However, as noted in Finding 3, the DoIT *Policy* did not provide complete guidance to State agencies for handling and reporting computer security instances. Consequently, certain State agencies that need to comply with security requirements of other oversight agencies may not achieve such compliance despite having complied with the DoIT *Policy*.

It should also be noted that agencies may not be aware of all security incidents. For example, OLA's regular audits of state agencies frequently find that agency security practices related to logging and reviewing security incidents need improvement. Of 135 audit reports issued by the OLA from July 2008 to January 2012, 34 reports, including all 5 reviewed in this audit, included findings and recommendations related to agency deficiencies in generating or reviewing security logs.

Confidential Information on Portable Devices

Finding 10

Confidential information contained on portable devices was not always properly protected.

Analysis

Certain State agencies did not take steps to adequately protect confidential information contained on portable devices (such as laptops) as well as any mobile devices (such as tablet computers and smart phones). DoIT *Policy* states that confidential information may not be stored on a State-owned portable device without prior approval and that approved storage must be encrypted.

Two of the five agencies tested (DHMH and DHR) did not implement practices (such as full disk encryption) designed to ensure that any confidential information contained on agency issued devices were protected from

disclosure in the event the device was lost or stolen. The number of portable devices containing confidential information was not determinable. The other three agencies (DPSCS, MVA, and the Comptroller) implemented procedures to encrypt such information.

To determine if agency issued laptops contained confidential information, we judgmentally selected 10 laptops issued to DHMH personnel according to DHMH records and asked the employee if 1) he or she used the laptop to access confidential information and 2) if such information were ever stored on the laptop. Three employees stated that they at times stored such information on the laptops.

As noted in Finding 4, while DoIT *Policy* includes a requirement that agencies approve the use of portable devices for storage of confidential information and the use of specified encryption technology, it does not address a number of other potential security issues or requirements.

Recommendation 10

We recommend that State agencies

- a. ensure that all confidential information contained on portable devices is encrypted as required by DoIT *Policy*, and
- b. develop a process to periodically verify that all portable devices hosting confidential information are properly protected.

Use of Certain Information Security Best Practices

Data Loss Prevention

Finding 11

State agencies were in various stages in implementing data loss prevention tools and techniques .

Analysis

Two of the five agencies we reviewed (Comptroller and DHR) had taken steps to implement data loss prevention (DLP) tools. Specifically, these agencies had taken steps to implement software products designed to monitor e-mail activity for certain patterns (such as data that resembles social security numbers) and flag such activity for further review. Our review at one of these agencies found that the DLP had resulted in the identification of suspicious e-mail activity that was subsequently investigated by the agency. The remaining

three agencies reviewed (DHMH, DPSCS, and MVA) had not investigated or implemented the use of DLP tools to protect agency data.

Recommendation 11

We recommend that State agencies

- a. **determine if implementation of DLP tools is appropriate and feasible based on agency data and resources (that is, benefits versus the related costs); and**
- b. **if appropriate, implement DLP tools and take appropriate action based on the related results.**

Vulnerability Scanning and Penetration Testing

Finding 12

State agencies had varied practices in implementing vulnerability scanning and penetration testing.

Analysis

Our review of the five State agencies disclosed that the agencies had implemented varying practices for vulnerability scanning and penetration testing. For example, we found that three agencies routinely performed vulnerability scanning for their information systems and reviewed the related results for remediation purposes, but that two agencies had not implemented any such practice. Furthermore, we found that two of these three agencies had performed penetration testing on certain information systems including one agency that routinely performed such testing.

Vulnerability scanning looks for specific vulnerabilities in a system and reports potential exposures. Such scans can generally be accomplished through an automated process. Penetration testing is designed to actually exploit weaknesses in a system and, therefore, requires various levels of expertise with the system. As a result, penetration testing is much more costly than vulnerability scanning and is also riskier since it can result in damage to the system.

(Note: Due to concerns expressed by certain agencies regarding the potential security implications associated with this finding, we have not identified the specific agencies and have not included responses to this finding in the Appendix, although such responses were previously provided to us.)

Recommendation 12

We recommend that State agencies, working in conjunction with DoIT

- a. develop and implement a vulnerability scanning process on a routine basis,**
- b. follow up on the vulnerability scanning results and take appropriate action to remediate vulnerabilities found,**
- c. determine the feasibility and need for performing penetration testing (based on cost and risk), and**
- d. perform penetration testing when indicated and take action on the related results.**

Appendix A

Glossary

Accreditation: The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations, agency assets, or individuals, based on the implementation of an agreed-upon set of security controls.

Cloud Computing: Using remote or Internet-based services and resources for data processing or data storage, with these services typically being provided via various communication channels by outside vendors on systems exclusively under the vendors' control.

Certification: A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

Confidential Information: Non-public information that if disclosed could result in a highly negative impact to the State of Maryland, its employees or citizens and may include information deemed as private, privileged, or sensitive.

Encryption: A process used to scramble data by applying a secret code so that no one can read the data without using a key.

Incident: An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

Information Security: The protection of information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

Availability (Security Objective): The disruption of access to or use of information or an information system results in a loss of availability.

Confidentiality (Security Objective): The unauthorized disclosure of information results in a loss of confidentiality.

Integrity (Security Objective): The unauthorized modification or destruction of information results in a loss of integrity.

Information System: A set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Penetration Testing: Security testing in which evaluators mimic real-world attacks in an attempt to identify ways to circumvent the security features of an application, system, or network. Penetration testing often involves issuing real attacks on real systems and data, using the same tools and techniques used by actual attackers. Most penetration tests involve looking for combinations of vulnerabilities on a single system or multiple systems that can be used to gain more access than could be achieved through a single vulnerability. In addition to taking advantage of technical holes in security, many penetration tests also use social engineering techniques to have insiders inappropriately disclose critical system features or access credentials (such as userids and passwords).

Personal Identifiable Information (PII): an individual's first name or initial and last name in combination with certain other information (for example, social security number).

Private Information: personally identifiable information (PII); such as an individual's social security number, financial or health records.

Privileged Information: records protected from disclosure by the doctrine of executive privilege which may include records:

- relating to budgetary and fiscal analyses, policy papers, and recommendations;
- relating to a State procurement when a final contract award has not been made or when disclosure of the record would adversely affect future procurement activity;
- of confidential advisory and deliberative communications relating to the preparation of management analysis projects.

Risk Management: The process of managing risks to organization operations (including mission, functions, images, or reputation), organizational assets, or individuals resulting from the operation of an information system and includes: 1) the conduct of a risk assessment, 2) the implementation of a risk mitigation strategy, and 3) employment of techniques and procedures for the continuous monitoring of the security state of the information system.

Security Assessment: The testing and/or evaluation of the management, operational, and technical security controls in an information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

Sensitive Information: information that if divulged, could compromise or endanger the citizens or assets of the State.

Vulnerability: Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Vulnerability Assessment: Formal evaluation and description of the vulnerabilities in an information system.

Vulnerability Scanning: A technique used to identify host and host attributes (such as operating systems, applications and open ports) and associated vulnerabilities. This is done by identifying operating systems and major software applications running on hosts and matching them with information on known vulnerabilities stored in the scanner vulnerability databases.

APPENDIX B



STATE OF MARYLAND
DEPARTMENT OF INFORMATION TECHNOLOGY

MARTIN O'MALLEY
Governor

ANTHONY BROWN
Lieutenant Governor

ELLIOT SCHLANGER
Secretary

September 18, 2012

Mr. Thomas J. Barnickel III, CPA
Acting Legislative Auditor
Office of Legislative Audits
301 West Preston Street
Room 1202
Baltimore, MD 21201

Dear Mr. Barnickel:

The Department of Information Technology (DoIT) has reviewed your draft audit report for DoIT and Selected State Agencies - Information System Data Security. As requested, our responses to the Findings 1 through 5 in the report are attached.

If you have any questions or need additional information, you may contact me at (410) 260-2994 or Elliot.Schlanger@maryland.gov.

A handwritten signature in black ink, appearing to read "Elliot H. Schlanger".

9/18/2012

Elliot Schlanger,
Secretary

Date

cc: Mr. Douglas Carrey-Beaver, Principal Counsel
Ms. Wendy Scott, Assistant Attorney General
Ms. Stacia Cropper, Chief Operating Officer
Mr. Greg Urban, Chief Technology Officer
Mr. Bruce Eikenberg, Director, Enterprise Information Services
Mr. Ron Witkowski, Chief Information Security Officer
Mr. Michael Powell, Chief Innovation Office, Executive Office of the Governor
Mr. Dick Ihrle, Compliance Auditor, Department of Budget and Management (DBM)
Ms. Joan Peacock, Manager, Audit Compliance Unit, DBM



Department of Information Technology (DoIT) Response to Legislative Audit Findings & Recommendations 1 – 5

Finding 1

Current State law governing certain protections for PII did not apply to State agencies and certain requirements established in State law also were not addressed in the DoIT *Policy*.

Recommendation 1

We recommend that DoIT

- a. propose legislation to address the protection of PII in the custody of State government agencies; and
- b. until such legislation is enacted, develop and implement a security breach notification policy containing requirements related to investigating system security breaches and notifying affected individuals and other parties as appropriate.

DoIT Response:

Concur

DoIT agrees that it is reasonable for State agencies to abide by the standards established in the Maryland Personal Information Protection Act (PIPA). Since this requirement does not yet exist in DoIT policy, DoIT concurs with this finding. Instead of proposing legislation, DoIT will accomplish the objective by adding PIPA compliance to the State Security policy.

DoIT will continue to update the Information Security Policy to reflect best practices and direct agencies to comply with the applicable sections of the Maryland Personal Information Protection Act. <http://www.oag.state.md.us/idtheft/businessGL.htm>. The next version of the Security policy will be published in November 2012 and will officially replace the existing policy in May 2013. This six month grace period gives agencies an opportunity to become familiar and compliant with the new policies.

Finding 2

DoIT did not have a formal process in place to monitor and enforce the provisions of its *Information Security Policy*.

Recommendation 2

We recommend that DoIT implement a process to monitor and enforce agency compliance with the *Policy*. For example, DoIT could consider requiring the use of an agency self-assessment tool as a means to help it ensure that State agencies have established comprehensive security programs

and conduct ongoing monitoring of security effectiveness. Results of the self-assessments could be submitted to and used by DoIT to assist in monitoring and enforcing agency compliance with the *Policy*.

DoIT's Response:

Oppose

DoIT agrees that additional monitoring and enforcement of agency compliance with the Policy would be beneficial. The responsibility for compliance, monitoring, and enforcement tasks are currently delegated to agencies. The example within the recommendation models the Federal approach. We agree this approach could be used to formalize DoIT's monitoring and enforcement process. This would require additional resources/ investments in software and staffing to manage reporting, analyze results, and develop recommendations. Until such time as DoIT has these resources, the current policy of delegating to the agencies is deemed the most appropriate way to ensure compliance with State security policy and will remain in effect.

Finding 3

DoIT could improve guidance to help agencies address certain security issues.

Recommendation 3

We recommend that DoIT review the comprehensiveness of its existing *Policy* guidance pertaining to the information security concepts and provide additional instruction or guidance as necessary to agencies for implementing components of agency security programs.

DoIT Response:

Concur

DoIT will update the existing policy to provide additional guidance by referencing recommendations in NIST SP 800-115 Technical Guide to Information Security Testing and Assessment, as well as NIST Special Publication 800-61 Computer Security Incident Handling Guide.

DoIT will further update the policy to describe the IT assistance that it can provide to agencies. This includes in-house expertise and the ability and authority to engage nationwide assistance from the Multi-State Information Sharing and Analysis Center and United States Computer Emergency Readiness Team.

DoIT will also recommend that agencies consider independent penetration testing to evaluate the effectiveness of their security program.

Finding 4

DoIT needs to develop a more responsive process to address emerging technologies as well as a policy regarding the security requirements for mobile devices.

Recommendation 4

We recommend that DoIT

- a. develop a process to more timely address the security implications of emerging technologies, and
- b. develop and issue a comprehensive statewide policy regarding minimum security requirements for mobile devices.

DoIT Response:

Concur

DoIT will issue periodic amendments to the Information Security Policy as new standards are developed to address emerging technologies and threats. As an example, guidance in the use of cloud-based Google Apps for Government was recently added to the State's Electronic Communication Policy. http://doit.maryland.gov/Publications/Electronic_Comm_Policy.pdf

Finding 5

DoIT had not developed recommended practices for implementing data loss prevention solutions.

Recommendation 5

We recommend that DoIT

- a. develop policy and guidance regarding the implementation of a data loss prevention strategy; and
- b. assist State agencies in researching, obtaining, and implementing data loss prevention tools.

DoIT Response:

Concur

Admittedly, the DoIT's Security Information Policy is not 'all inclusive'. The Policy does require agencies to establish an Agency Security Program. In the course of developing such a program, an agency may determine that a data loss prevention (DLP) system is applicable or appropriate. The risk of confidential data leakage can be greatly mitigated by implementing many of the requirements (security controls) within the existing Information Security Policy. This includes properly marking confidential data, categorizing their systems, identifying all access paths to confidential data, providing an enterprise solution for secure data exchange, and educating users on proper handling of data.



We agree a DLP solution is a tool that can be used to enforce a data loss policy. A DLP solution could only be cost effective if, after implementation of recommended security controls, the risk of data loss still remains at an unacceptable level for the agency. DoIT will add an overview to essential capabilities of a DLP in the next version of the Security Policy.

Providing assistance to agencies in researching, obtaining, and implementing DLP tools would require additional skilled resources. Until such time as DoIT has these resources, the responsibility to select, obtain, and implement a DLP solution remains with the agency.



Peter Franchot
Comptroller

Linda L. Tanton
Deputy Comptroller

September 12, 2012

Mr. Thomas J. Barnickel III, CPA
Acting Legislative Auditor
Department of Legislative Services
301 West Preston St., Room 1202
Baltimore, MD 21201

Dear Mr. Barnickel,

Enclosed is the Comptroller's response to your letter dated August 29, 2012 with the Comptroller of Maryland's (COM) portion of the performance audit report on the Department of Information Technology and Selected State Agencies.

We have carefully reviewed each finding, and we believe that the attached responses fully address each recommendation contained in the report. Should you need additional information or clarification, please contact Karen Tobat, Compliance Manager, Internal Audit Division by email at ktobat@comp.state.md.us or by telephone at 410.260.7598.

The Comptroller appreciates your objective appraisal of our operations and your recommendations for continuous improvement.

Very truly yours,

Linda L. Tanton
Deputy Comptroller

Lavinia Lee
Director, Information Technology Division

Cc: Honorable Peter V.R. Franchot, Comptroller
Michelle Bohlayer, Acting Director, Internal Audit Division, COM
Karen Tobat, Compliance Manager, Internal Audit Division, COM
David Hildebrand, Supervisor of Security and Internet Services, COM
Steven Barzal, Director, Office of Human Resources, COM

Risk Management Process

Finding 8 – Risk management processes were not fully implemented.

Auditor's Recommendation:

We recommend that State agencies

- a. develop and document a risk management process including risk assessments that apply to all critical systems,
- b. specify how frequently risk assessments should be re-evaluated,
- c. perform risk assessments for all critical systems currently in use, and
- d. periodically update or re-evaluate the risk assessments.

Comptroller of Maryland (COM) Response:

The COM agrees with the auditor's recommendations.

- a. The COM Information Technology Division will develop and document a risk management process for all critical systems. Concepts identified in the Federal Information Processing Standards (FIPS) 199 will be applied to the document. The risk management process document will identify all critical systems and assign a level of criticality and sensitivity (i.e. security categorization) based on confidentiality, integrity, and availability.
- b. The risk management process document will require periodic re-evaluation of risk assessments. The re-evaluation period to be dependent on the system security categorization. High impact systems will require re-evaluation of risk assessments every two (2) years. Moderate impact systems will require re-evaluation of risk assessments every four (4) years.
- c. The COM will perform risk assessments for all critical systems in use. As stated in the performance audit report, the COM has completed a risk assessment for the Annapolis Data Center (ADC), which is responsible for serving multiple State Agencies. The COM is currently completing a risk assessment for the State of Maryland's Tax System (SMART). In addition, the COM completed a preliminary Certification and Accreditation review of four new systems (Teradata Data Warehouse, Business Objects, ETL Server, and the Case Management System) in January 2010. A final Certification and Accreditation review will be completed by October 31, 2012 for these four systems, plus two additional systems (SAS and BizTalk).
- d. Please see "b" above.

Effective Completion Date: The documented risk management process will be completed by December 31, 2012. Based on the assessed security categorization of each system, risk assessments for critical systems will be completed in phases. Initial risk assessments for all high impact systems to be completed by March 2014.

Security Awareness Program

Finding 9 – Security awareness training was not always provided to employees or tracked.

Auditor's Recommendation:

We recommend that agencies provide timely security awareness training to all employees and document employee attendance at the training.

Comptroller of Maryland (COM) Response:

The COM agrees with the auditor's recommendation. The COM has a comprehensive security awareness training program. All employees with access to confidential data are required to obtain annual security awareness training that complies with IRS Publication 1075 requirements. Previously, each COM Division tracked their employee's training. The two largest divisions (Revenue Administration and Compliance) hold mandatory professional development sessions each Fall. Employees certify attendance to the security awareness portion of the training. The COM's Information Technology Division offers security awareness training to all COM employees throughout the year. To strengthen compliance, tracking of employee training will be centralized within the COM's Office of Human Resources (OHR) effective September 30, 2012.

Effective Completion Date: September 30, 2012.



STATE OF MARYLAND

DHMH

Maryland Department of Health and Mental Hygiene

201 W. Preston Street • Baltimore, Maryland 21201

Martin O'Malley, Governor – Anthony G. Brown, Lt. Governor – Joshua M. Sharfstein M.D., Secretary

September 17, 2012

Mr. Thomas J. Barnickel III, CPA
Acting Legislative Auditor
Office of Legislative Audits
301 West Preston Street
Baltimore, MD 21201

Dear Mr. Barnickel:

Thank you for your letter regarding the draft performance audit report on the Department of Information Technology and Selected State Agencies – Information System Data Security which included the Department of Health and Mental Hygiene. Enclosed you will find the Department's response and plan of correction that addresses each audit recommendation pertaining to this Department - Findings 6, 8, 9, 10 and 11. I will work with the Chief Information Officer and Deputy Secretary to promptly address the audit exceptions. In addition, the Office of Inspector General's Division of Internal Audits will follow-up on the recommendations to ensure compliance.

If you have any questions or require additional information, please do not hesitate to contact Thomas V. Russell of my staff at (410) 767-5862.

Sincerely,

Joshua M. Sharfstein, M.D.
Secretary

Enclosure

cc: Thomas Kim, Deputy Secretary for Operations, DHMH
Patrick D. Dooley, Chief of Staff, Office of the Secretary, DHMH
Thomas V. Russell, Inspector General, DHMH
Ellwood L. Hall, Jr., Assistant Inspector General, DHMH
Lisa J. Ellis, Chief Administrative Officer, DHMH
Saleem Sayani, Chief Information Officer, DHMH

Toll Free 1-877-4MD-DHMH • TTY/Maryland Relay Service 1-800-735-2258

Web Site: www.dhmh.state.md.us



Audit Finding 6:

System Categorization: State agencies often did not document the security categorization of their information systems.

Recommendation 6:

We recommend that State agencies comply with DoIT *Policy* by evaluating and documenting security categories for all of their information systems and establish security measures commensurate with data sensitivity and risk.

Administration's Response:

We concur with the findings and recommendations. OIT is in the process of implementing System Security assessments and security plans using NIST 800-53 as our guiding document. An important part of this process is assigning all systems a security category using FIPS Publication 199 as guidance. This categorization and assessment process will meet the state IT security requirements and categorize our systems based on potential impact on an agency should certain events occur which jeopardize the information and information systems.

Timeline for compliance: System assessment and categorization is in process for all listed systems and is expected to be completed by June 2013.

**Audit Finding 8:
Risk management**

**Finding 8
Risk management processes were not fully implemented.**

Auditor's Recommendation:

We recommend that State agencies

- a. develop and document a risk management process including risk assessments that apply to all critical systems,**
- b. specify how frequently risk assessments should be re-evaluated,**
- c. perform risk assessments for all critical systems currently in use, and**
- d. periodically update or re-evaluate the risk assessments.**

Administration's Response:

We concur with the finding and recommendations. (a) OIT is in the process of preparing System Security assessments and security plans for critical systems using NIST 800-53 as our guiding document, (b) the initial assessment is to be followed by a re-assessment annually, or if required by incident or modification, (c) all current operational systems categorized as "critical" will be assessed, and (d) this formal re-evaluation process, by agency policy, is annually at a minimum, or as required by incident or modification

Timeline for compliance:

Because this process is resource intensive, we have broken up this effort into two phases. System assessment is in process for systems deemed critical, as a first phase approach, which is expected to be completed by June 2013. A second phase which will assess and prepare mitigation plans for the other non-critical systems is expected to be completed by January 2014.

Security Awareness Program

Finding 9

Security awareness training was not always provided to employees or tracked.

Auditor's Recommendation:

We recommend that agencies provide timely security awareness training to all employees and document employee attendance at the training.

Administration's Response:

We concur with the finding and fully agree with the recommendation.

Currently, DHMH does provide the mandatory IT Security awareness training to all new hires in our employee orientation. A listing of all employees trained is maintained.

We also provide an on-line training accessible to all employees, however, cost and complexity to develop a separate tracking system for over 9,000 employees at multiple statewide locations have to date made this unreachable.

Timeline for Compliance:

By January 2013, working closely with our Office of Human Resources who is responsible for the implementation of mandatory training, we plan to implement an on-line, web-based training and tracking system.

Confidential Information on Portable Devices

Finding 10

Confidential information contained on portable devices was not always properly protected.

Recommendation 10

We recommend that State agencies

- a. ensure that all confidential information contained on portable devices is encrypted as required by DoIT *Policy*, and
- b. develop a process to periodically verify that all portable devices hosting confidential information are properly protected.

Administration's Response:

We concur with the finding and recommendations and note that in the review process no confidential information was discovered on the ten laptops reviewed.

(a) DHMH requires by IT Security policy (02.01.01) - which includes laptops and removable media, all agency units to strictly control the usage of PHI on all removable devices and media (including laptops), we are installing end-point protection software on all hard drives, laptops, and removable media throughout the agency,

(b) due to personnel limitations and responsibility for procurement and inventory, OIT was not able to routinely spot-check these devices and assure these practices. With the recent completion of Service Level Agreements with key DHMH business units and staff reassignment, OIT gains the necessary staff to implement such an assurance program.

Additionally to technically enforce implementation of this administrative policy

Timeline for compliance:

(a) A laptop and removable media PHI protection process was implemented as a pilot phase approach in September 2012,

(b) a fully implemented protection and inspection process in coordination with the agency Office of Corporate Compliance is expected to be in place by January 2013.

Data Loss Prevention

Finding 11

State agencies were in various stages in implementing data loss prevention tools and techniques .

Recommendation 11

We recommend that State agencies

- a. determine if implementation of DLP tools is appropriate and feasible based on agency data and resources (that is, benefits versus the related costs); and**
- b. if appropriate, implement DLP tools and take appropriate action based on the related results.**

Administration's Response:

We partially concur with the finding and fully agree with the recommendation. We currently have the IronPort security appliance in place which provides a range of services including limited key data element scanning. Additionally, our recent migration to the State Email system (Google - Maryland.gov) provides spam protection and enhanced email security services.

(a) DHMH continues to operate network intrusion detection/prevention systems and explore and assess additional DLP services which might be available under the Google Government Apps services, (b) if feasible and warranted, our agency may implement additional DLP capabilities.

Timeline for Compliance:

Potential implementation of a more advanced DLP email solution is dependent on the full, tested implementation and expanded capabilities of the statewide email system (estimated end of 2012), or through the use of third party applications, and is contingent on our risk assessment and budget considerations.



Department of Public Safety and Correctional Services

Office of the Secretary

300 E. JOPPA ROAD • SUITE 1000 • TOWSON, MARYLAND 21286-3020
(410) 339-5000 • FAX (410) 339-4240 • TOLL FREE (877) 379-8636 • V/TTY (800) 735-2258 • www.dpscs.maryland.gov

September 13, 2012

STATE OF MARYLAND

MARTIN O'MALLEY
GOVERNOR

ANTHONY G. BROWN
LT. GOVERNOR

GARY D. MAYNARD
SECRETARY

G. LAWRENCE FRANKLIN
DEPUTY SECRETARY
ADMINISTRATION

J. MICHAEL STOUFFER
DEPUTY SECRETARY
OPERATIONS

RHEA L. HARRIS
ASSISTANT SECRETARY/
CHIEF OF STAFF

DAVID N. BEZANSON
ASSISTANT SECRETARY
CAPITAL PROGRAMS

JON P. GALLEY
DIRECTOR
NORTHERN REGION

WENDELL M. FRANCE
DIRECTOR
CENTRAL REGION

PATRICIA VALE
DIRECTOR
SOUTHERN REGION

PATUXENT INSTITUTION

MARYLAND COMMISSION
ON CORRECTIONAL
STANDARDS

MARYLAND POLICE &
CORRECTIONAL TRAINING
COMMISSION

MARYLAND PAROLE
COMMISSION

CRIMINAL INJURIES
COMPENSATION BOARD

EMERGENCY NUMBER
SYSTEMS BOARD

SUNDRY CLAIMS BOARD

INMATE GRIEVANCE OFFICE

Mr. Thomas J. Barnickel III, CPA
Acting Legislative Auditor
Office of Legislative Audits, Room 1202
301 West Preston Street
Baltimore, MD 21201

Dear Mr. Barnickel:

The Department of Public Safety and Correctional Services has reviewed the draft performance audit report dated August 29, 2012 for the Department of Information Technology and Selected Agencies – Information System Data Security. The Department appreciates the constructive recommendations that were made as the result of this audit.

Attached is Chief Information Officer Brothers' response to the draft performance audit report, with which I concur. Mr. Brothers will continue to implement corrective action to address the findings and recommendations related to the Department, and will closely monitor the status in order to prevent any repeat audit findings in the next audit.

I trust that these responses adequately address the relevant findings and recommendations contained in the draft performance audit report. If you have any questions regarding the Department's responses, please contact me.

Sincerely,

Gary D. Maynard
Secretary

Attachment

Cc: G. Lawrence Franklin, Deputy Secretary for Administration, DPSCS
Ronald C. Brothers, Chief Information Officer, ITCD
Joseph M. Perry, Inspector General, DPSCS



Department of Public Safety and Correctional Services

Information Technology & Communications Division

Post Office Box 5743 • Pikesville, Maryland 21282-5743
Main No: 410-585-3100 • Facsimile No: 410-764-4035 • www.dpscs.state.md.us

STATE OF MARYLAND

MARTIN O'MALLEY
GOVERNOR

ANTHONY G. BROWN
LT. GOVERNOR

GARY D. MAYNARD
SECRETARY

G. LAWRENCE FRANKLIN
DEPUTY SECRETARY
ADMINISTRATION

J. MICHAEL STOUFFER
DEPUTY SECRETARY
OPERATIONS

DAVID N. BEZANSON
ASSISTANT SECRETARY
CAPITAL PROGRAMS

RONALD C. BROTHERS
CHIEF INFORMATION
OFFICER

C. KEVIN COMBS
DEPUTY CHIEF
INFORMATION OFFICER

September 12, 2012

Gary D. Maynard, Secretary
Department of Public Safety & Correctional Services
300 East Joppa Road, Suite 1000
Towson, Maryland 21286

Via

G. Lawrence Franklin, Deputy Secretary
Department of Public Safety & Correctional Services
300 East Joppa Road, Suite 1000
Towson, Maryland 21286

Dear Secretary Maynard:

Enclosed is the Information Technology and Communications Division's (ITCD) response to the OLA's August 29, 2012 draft performance audit report on the Department of Information Technology and Selected State Agencies – Information System Data Security. This audit included a review of the Department's policies and practices for compliance with certain elements of the 2010 Policy that would help secure information systems and related data. The Department has begun, and will continue to pursue full implementation of all of the legislative auditor's recommendations.

Finding 6:

State agencies often did not document the security categorization of their information systems.

Recommendation 6:

We recommend that State agencies comply with DoIT Policy by evaluating and documenting security categories for all of their information systems and establish security measures commensurate with data sensitivity and risk.

We agree

DPSCS is in the process of categorizing system security levels to all critical systems in compliance with DoIT data sensitivity classifications. System security categorization has begun which will allow for more accurate risk assessment documentation. The anticipated completion for documenting security categories is March 2013 and for establishing security measures is April 2014.

Finding 7:

Certain agencies' information security policies were not agency specific or did not include all required components.

Recommendation 7:

We recommend that State agencies develop an agency-specific information security policy that addresses the required components of an overall information security program established by the DoIT Policy.

9.17.12

OK
SLF

We agree

DPSCS is in the process of evaluating systems missing required components of the security policy. Furthermore, an evaluation of systems that require certification and accreditation in accordance with DoIT Information Security Policy has started and the anticipated completion date is December 2013.

Finding 8:

Risk management processes were not fully implemented.

Recommendation 8:

We recommend that State agencies

- a. **develop and document a risk management process including risk assessments that apply to all critical systems,**
- b. **specify how frequently risk assessments should be re-evaluated,**
- c. **perform risk assessments for all critical systems currently in use, and**
- d. **periodically update or re-evaluate the risk assessments.**

We agree

DPSCS is in the process of categorizing system security levels to all critical systems and adding more documentation for systems in compliance with DoIT data sensitivity classifications. This process will allow for a more accurate risk analysis of the critical systems. Risk assessment evaluations are planned to be conducted tri-annually to re-evaluate and update documentation. The anticipated completion date is June 2014.

Finding 11:

State agencies were in various stages in implementing data loss prevention tools and techniques.

Recommendation 11:

We recommend that State agencies

- a. **determine if implementation of DLP tools is appropriate and feasible based on agency data and resources (that is, benefits versus the related costs); and**
- b. **if appropriate, implement DLP tools and take appropriate action based on the related results.**

We agree

DPSCS has acquired the Checkpoint DLP software solution and anticipates implementing it by January 2013.

Please advise if you have any questions regarding the Division's responses to the audit report.

Sincerely,



Ronald C. Brothers
Chief Information Officer

RCB:tdp

c: G. Lawrence Franklin, Deputy Secretary
Joseph M. Perry, Inspector General
File

Martin O'Malley
Governor

Anthony Brown
Lt. Governor

Theodore Dallas
Secretary

September 17, 2012

Mr. Thomas J. Barnickel, CPA
Acting Legislative Auditor
State of Maryland – Office of Legislative Audits
State Office Building, Room 1202
301 West Preston Street
Baltimore, MD 21201

Dear Mr. Barnickel:

Thank you for the opportunity to respond to the audit findings and recommendations from the draft performance report on the Department of Information Technology and Selected State Agencies – Information System Data Security. As requested, enclosed please find the Department's response and plan of correction that addresses the audit recommendations for Findings 6 through 10.

If you have any questions or require additional information, please contact Mr. William E. Johnson, Jr., Inspector General, at 443-378-4060 or wjohnson@dhr.state.md.us.

Sincerely,



Theodore Dallas
Secretary

Enclosure

cc: ML Wermecke, Chief of Staff, DHR
Leonard James Howie, III, Deputy Secretary, DHR
Thomasina Hiers, Deputy Secretary, DHR
William E. Johnson, Jr., Inspector General, DHR
Kenyetta Powers, Interim Chief Information Officer, DHR

Department of Human Resources
Department of Information Technology and Selected State Agencies – Information System Data
Security
Response to Draft Audit Report

Finding 6

State agencies often did not document the security categorization of their information systems.

Recommendation 6

We recommend that State agencies comply with DoIT *Policy* by evaluating and documenting security categories for all of their information systems and establish security measures commensurate with data sensitivity and risk.

Department's Response

The Department of Human Resources (hereafter, DHR or the Department) agrees with the recommendation and has completed the security categorization of their information systems.
Completed 6/4/2012

Finding 7

Certain agencies' information security policies were not agency specific or did not include all required components.

Recommendation 7

We recommend that State agencies develop an agency-specific information security policy that addresses the required components of an overall information security program established by the DoIT *Policy*.

Department's Response

The Department agrees with the recommendation and has created Agency specific policy that addresses Certification and Accreditation.
Completed 6/1/2012

Finding 8

Risk management processes were not fully implemented.

Recommendation 8

We recommend that State agencies

- a. develop and document a risk management process including risk assessments that apply to all critical systems,
- b. specify how frequently risk assessments should be re-evaluated,
- c. perform risk assessments for all critical systems currently in use, and
- d. periodically update or re-evaluate the risk assessments.

Department's Response

The Department agrees with the recommendations and will use the findings, recommendations and other referenced materials as a guideline for implementing a Risk Management Process that includes the Information Systems as well as the Data Center. The following corrective actions will be implemented:

- 1) Create a Risk Assessment policy - Completed 6/1/2012
- 2) Perform Risk Assessments that include the Agency's critical systems and prioritize the efforts according to security categorization.
Implementation Date: 3/1/2013

Finding 9

Security awareness training was not always provided to employees or tracked.

Recommendation 9

We recommend that agencies provide timely security awareness training to all employees and document employee attendance at the training.

Department's Response

The Department agrees with the recommendation and will implement the following corrective actions:

- 1) Update and refresh Agency specific and general security policy and training materials.
Implementation Date: 11/1/2012
- 1) Create policy and process to assure that employees are attending security awareness training.
Implementation Date: 1/2/2013

Finding 10

Confidential information contained on portable devices was not always properly protected.

Recommendation 10

We recommend that State agencies

- a. ensure that all confidential information contained on portable devices is encrypted as required by DoIT *Policy*, and
- b. develop a process to periodically verify that all portable devices hosting confidential information are properly protected.

Department's Response

The Department agrees with the recommendations and will implement the following corrective actions:

- 1) Create system capable of managing portable media encryption hardware needs.
Completed: 8/22/2012
- 2) Perform Statewide implementation of encryption management system.
Implementation Date: 2/22/2013



Maryland Department of Transportation
The Secretary's Office

Martin O'Malley
Governor

Anthony G. Brown
Lt. Governor

Darrell B. Mobley
Acting Secretary

Leif A. Dormsjo
Acting Deputy Secretary

September 14, 2012

Thomas J. Barnickel III, CPA
Acting Legislative Auditor
Office of Legislative Audits
Department of Legislative Services
Room 1202
301 West Preston Street
Baltimore MD 21201

Dear Mr. Barnickel:

Enclosed please find the Department's responses to the Office of Legislative Audits' Draft Performance Audit Report dated August 2012, on Department of Information Technology and Selected State Agencies. Additionally, an electronic version of this document has been sent to your office via email at response@ola.state.md.us (file name: DataSecurityPerformanceReportFindings6-8-9-11).

If you have any questions or need additional information, please do not hesitate to contact me or Mr. David L. Fleming, Chief Financial Officer. Mr. Fleming can be reached at 410-865-1035.

Sincerely,

Darrell B. Mobley
Acting Secretary

Enclosure

cc: Mr. Rick A. Bilenky, Chief Internal Auditor, Motor Vehicle Administration
Mr. Chuck Bristow, Chief Information Officer, Maryland Department of Transportation
Mr. Milton Chaffee, Chief Deputy Administrator, Motor Vehicle Administration
Mr. Leif Dormsjo, Acting Deputy Secretary, Maryland Department of Transportation
Mr. David L. Fleming, Chief Financial Officer, Maryland Department of Transportation
Mr. John T. Kuo, Administrator, Motor Vehicle Administration
Mr. Guy Reihl, Director, Office of Transportation Technology Services, Maryland Department of Transportation
Ms. Lisa Rosenberg, Acting Director, Office of Audits, Maryland Department of Transportation
Mr. Al Short, Chief Information Officer, Motor Vehicle Administration

**Maryland Department of Transportation
Motor Vehicle Administration
Performance Audit
Department of Information Technology and Selected State Agencies –
Information System Data Security
August 2012**

Security Categorization of Information Systems

Finding 6

State agencies often did not document the security categorization of their information systems.

Recommendation 6

We recommend that State agencies comply with DoIT Policy by evaluating and documenting security categories for all of their information systems and establish security measures commensurate with data sensitivity and risk.

Response 6

The Maryland Department of Transportation (Department) and the Motor Vehicle Administration (MVA) concur with the recommendation, and have reviewed all MVA applications and documented the security categories. This MVA review was completed June 19, 2012. Security measures will be documented in the safeguard implementation plans as a result of risk assessments of critical systems commensurate with data sensitivity and risk.

Risk Management Process

Finding 8

Risk management processes were not fully implemented.

Recommendation 8

We recommend that State agencies

- a. develop and document a risk management process including risk assessments that apply to all critical systems,**
- b. specify how frequently risk assessments should be re-evaluated,**
- c. perform risk assessments for all critical systems currently in use, and**
- d. periodically update or re-evaluate the risk assessments.**

Maryland Department of Transportation
Motor Vehicle Administration
Performance Audit
Department of Information Technology and Selected State Agencies –
Information System Data Security
August 2012

Response 8

The Department concurs and will re-visit the Safeguard implementation plan, Section 16 of the MDOT Security Plan and determine what, if any, additions have to be made to accommodate system risk assessments. Section 16 was developed using best practices recommended by NIST standard SP 800-30. The review and update of the policy, if needed, will include:

- A standard process for performing risk assessments of critical systems
- A standard process for determining the appropriate department or agency to perform a specific risk assessment
- A schedule solicited from all of the MDOT Transportation Business Units (TBU) of when their specific initial system risk assessments are completed
- Guidance for the regularity of the re-evaluation of the TBU risk assessments.

The review and any changes to Section 16 of the MDOT Security Plan shall be completed by June 2013.

Security Awareness Program

Finding 9

Security awareness training was not always provided to employees or tracked.

Recommendation 9

We recommend that agencies provide timely security awareness training to all employees and document employee attendance at the training.

Response 9

The Department and MVA concur with the recommendation. The MVA Organizational Development (OD) division makes security awareness training available to all existing and new employees through the Learning Management System (LMS) and requests that all new employees take this training during the first 60 days of hire. Respective managers and division heads will ensure that new employees complete the security awareness training within 60 day of hire as required. Respective managers and division heads will also ensure that existing employees complete the security awareness training by June 30, 2013. Furthermore, a security awareness program shall be implemented for MDOT. The content of such program will be established and distributed by June 2013.

**Maryland Department of Transportation
Motor Vehicle Administration
Performance Audit
Department of Information Technology and Selected State Agencies –
Information System Data Security
August 2012**

Data Loss Prevention

Finding 11

State agencies were in various stages in implementing data loss prevention tools and techniques.

Recommendation 11

We recommend that State agencies

- a. determine if implementation of DLP tools is appropriate and feasible based on agency data and resources (that is, benefits versus the related costs); and**
- b. if appropriate, implement DLP tools and take appropriate action based on the related results.**

Response 11

The Department and the MVA concur with the recommendations and will conduct an analysis and eventual implementation of a Data Loss Prevention Program. Given the likely necessity to conduct a procurement to fully implement such a program, and the potential impact to MDOT operations, this implementation will be initially limited to MVA. The initial implementation will be a model used as a baseline for a Department-wide implementation. The analysis effort shall be completed by January 1, 2013. After the analysis is complete, an implementation plan and schedule shall be created. This will be the mutual responsibility of a designee of the MVA and a designee from MDOT.

AUDIT TEAM

Edward L. Shulder, CPA
Audit Manager

Amber M. Schon, CPA, CFE
Senior Auditor

Marissa L. Eby
Staff Auditor