Audit Report

State Retirement Agency

December 2014

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

Thomas J. Barnickel III, CPA
Legislative Auditor

December 22, 2014

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 have conducted a fiscal compliance audit of the State Retirement Agency for the period beginning May 20, 2011 and ending April 1, 2014. The Agency provides administrative support services and investment functions for the State Retirement and Pension System of Maryland, a cost-sharing multiple-employer public employee retirement system.

Our audit disclosed that sufficient procedures were not established for reviewing certain activities occurring in the Agency's automated system used to calculate and process retirement and pension benefits for retirees and beneficiaries and contributions for current members. As a result, unauthorized activities could go undetected that could adversely affect the integrity of the system. We also noted that the intrusion detection prevention system was not properly configured to protect the Agency's network.

The Agency's response to this audit is included as an appendix to this report. We wish to acknowledge the cooperation extended to us during the course of this audit by the Agency.

Respectfully submitted,

Thomas J. Barnickel III, CPA
Legislative Auditor

301 West Preston Street · Room 1202 · Baltimore, Maryland 21201
410-946-5900/301-970-5900 · Fax 410-946-5999/301-970-5999
Toll Free in Maryland 877-486-9964 · Fraud Hotline 877-FRAUD-11

Background Information

Agency Responsibilities

The State Retirement Agency provides administrative support services and investment functions for the State Retirement and Pension System (System) of Maryland, a cost-sharing multiple-employer public employee retirement system consisting of a State pool and a Municipal pool. The State pool includes State agencies, boards of education, community colleges, and libraries, while the Municipal pool includes participating local governmental units that elected to join the System. The System was established by the State Personnel and Pensions Article of the Annotated Code of Maryland and comprises the following individual systems: Teachers' Retirement and Pension Systems, Employees' Retirement and Pension Systems, State Police Retirement System, Judges' Retirement System, and the Law Enforcement Officers' Pension System. Responsibility for the administration and operation of the System is vested in a 15-member Board of Trustees. According to the State's records, the Agency's operating expenditures totaled approximately $26.2 million during fiscal year 2013.

Financial Statement Audits

For fiscal years 2013 and 2012, the Agency engaged an independent accounting firm to perform the audit of the System's financial statements. The firm expressed an opinion that the System's financial statements presented fairly, in all material respects, the respective financial position of the System as of June 30, 2013 and 2012, and the changes in plan net position for the years then ended, in conformity with accounting principles generally accepted in the United States of America.

Select System Financial Information

According to its records, as of June 30, 2013, the System had approximately 138,000 retirees and beneficiaries, and approximately 193,000 active participants. The following table provides select System financial information.

Select System Financial Information					
Fiscal Year	**Total Contributions**	**Net Investment Income**	**Benefit Payments**	**Total Net Position at June 30**	**Unfunded Actuarial Accrued Liability**
2013	$2.4 billion	$3.8 billion	$3.0 billion	$40.4 billion	$20.7 billion
2012	$2.3 billion	$0.1 billion	$2.8 billion	$37.2 billion	$20.6 billion

Source: Audited System Financial Statements

Note: The Unfunded Actuarial Accrued Liability is the amount by which the Actuarial Accrued Liability exceeds the Actuarial Value of Assets as determined by the System's actuary.

Status of Findings From Preceding Audit Report

Our audit included a review to determine the status of the finding contained in our preceding audit report dated March 2, 2012. We determined that the Agency satisfactorily addressed this finding.

Findings and Recommendations

Information Systems Security and Control

Background

The State Retirement Agency hosts the Maryland Pension Administration System (MPAS). MPAS is a server-based application that calculates and processes retirement and pension benefits for retirees and beneficiaries and contributions for current members. The Agency's wide area network provides employee access to various information technology services including business productivity applications, database management systems, network file and print services, email services, Internet access, and connectivity to State of Maryland hosted mainframe systems.

Finding 1
The Agency's procedures for reviewing certain critical security events were not sufficient.

Analysis
The Agency's procedures for reviewing certain critical security events were not sufficient.

- Although the Agency reviewed certain MPAS database security-related events, other critical security events (grant, revoke, and deny database access), audit events (add audit, modify audit, and stop audit), and direct modifications to critical tables (insert, update, and delete) were not reviewed for propriety. Accordingly, significant database security events, audit events, and direct modifications to critical tables could go undetected, thus permitting unauthorized or inappropriate activities to adversely affect the integrity of the MPAS production database.

- Although the Agency logged critical MPAS application server security events, the Agency did not have documentation to support that reviews of these logged events were performed. Accordingly, unauthorized or inappropriate activities affecting the integrity of the MPAS application server could go undetected by management.

The State of Maryland Department of Information Technology's (DoIT) *Information Security Policy* requires that information systems must generate audit records for all security-relevant events, including all security and system administrator accesses. The *Policy* also requires that procedures be developed to routinely (for example daily or weekly) review audit records for indications of unusual activities, suspicious activities or suspected violations, and report findings to appropriate officials for prompt resolution.

Recommendation 1
We recommend that the Agency
a. review critical MPAS database and server security events, audit events, and direct modifications to critical tables;
b. document these reviews; and
c. retain the documentation for future reference.

Finding 2
The Agency's intrusion detection prevention system was not properly protecting the network.

Analysis
The Agency's intrusion detection prevention system (IDPS) was not properly protecting the network.

- The Agency did not use IDPS on 11 critical servers that processed encrypted traffic. The Agency headquarters' firewall and its integrated intrusion prevention system (IPS) component included the capability to decrypt inbound encrypted traffic and to subject such traffic to IPS processing. However, the firewall was not configured to use this feature.

- Although the Agency used a network-based IDPS to monitor unencrypted traffic, the IDPS was not properly configured and, as a result, traffic to two critical servers was not subject to IDPS coverage.

Properly configured IDPS protection can aid significantly in the detection/prevention of, and response to, potential network security breaches and attacks. Furthermore, without proper IDPS monitoring, critical network security breaches may occur that could otherwise possibly be detected and prevented.

Recommendation 2
We recommend that the Agency perform a documented review and assessment of its network security risks and identify how IDPS coverage should be best applied to its network and inbound encrypted traffic. Based on this review and assessment, we recommend that the Agency implement IDPS coverage as necessary.

Audit Scope, Objectives, and Methodology

We have conducted a fiscal compliance audit of the State Retirement Agency for the period beginning May 20, 2011 and ending April 1, 2014. The audit was conducted 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.

As prescribed by the State Government Article, Section 2-1221 of the Annotated Code of Maryland, the objectives of this audit were to examine the Agency's financial transactions, records and internal control, and to evaluate its compliance with applicable State laws, rules, and regulations.

In planning and conducting our audit, we focused on the major financial-related areas of operations based on assessments of significance and risk. The areas addressed by the audit included benefits paid to retirees and beneficiaries, contributions required from participating employers, critical information systems, purchases and disbursements, and payroll. We also determined the status of the finding included in our preceding audit report.

To accomplish our objectives, our audit procedures included inquiries of appropriate personnel, inspections of documents and records, observations of the Agency's operations, and tests of transactions. We also performed various data extracts of pertinent information from the State's Financial Management Information System (such as revenue and expenditure data) and the State's Central Payroll Bureau (payroll data). The extracts are performed as part of ongoing internal processes established by the Office of Legislative Audits and were subject to various tests to determine data reliability. We determined that the data extracted from these various sources were sufficiently reliable for the purposes the data were used during this audit. We also extracted data from the Agency's automated Maryland Pension Administration System for the purpose of testing pension contributions and benefits. Finally, we performed other auditing procedures that we considered necessary to achieve our audit objectives. The reliability of data used in this report for background or informational purposes was not assessed.

The Agency's management is responsible for establishing and maintaining effective internal control. Internal control is a process designed to provide reasonable assurance that objectives pertaining to the reliability of financial records, effectiveness and efficiency of operations including safeguarding of assets, and compliance with applicable laws, rules, and regulations are achieved.

Because of inherent limitations in internal control, errors or fraud may nevertheless occur and not be detected. Also, projections of any evaluation of internal control to future periods are subject to the risk that conditions may change or compliance with policies and procedures may deteriorate.

Our reports are designed to assist the Maryland General Assembly in exercising its legislative oversight function and to provide constructive recommendations for improving State operations. As a result, our reports generally do not address activities we reviewed that are functioning properly.

This report includes conditions that we consider to be significant deficiencies in the design or operation of internal controls that could adversely affect the Agency's ability to operate effectively and efficiently, and/or comply with applicable laws, rules, and regulations. These conditions also represent significant instances of noncompliance with applicable laws, rules, or regulations. Other less significant findings were communicated to the Agency that did not warrant inclusion in this report.

The Agency's response to our findings and recommendations is included as an appendix to this report. As prescribed in the State Government Article, Section 2-1224 of the Annotated Code of Maryland, we will advise the Agency regarding the results of our review of its response.

APPENDIX

MARYLAND
STATE RETIREMENT
and PENSION SYSTEM

STATE RETIREMENT AGENCY
120 East Baltimore Street
Baltimore, MD 21202
Tel: 410-625-5555
1-800-492-5909
TDD/TTY 410-625-5535
sra.maryland.gov

R. Dean Kenderdine
Executive Director
Secretary To The Board

December 19, 2014

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

Dear Mr. Barnickel:

Enclosed, please find the Maryland State Retirement Agency's response to the draft audit report for the period beginning May 20, 2011 and ending April 1, 2014.

In accordance with the Joint Audit Committee's *Policy on Agency Responses to Reports Issued by the Office of Legislative Audits,* enclosed please find the State Retirement Agency's response as required.

If you should have any questions regarding our response, please feel free to contact me.

Sincerely,

R. Dean Kenderdine
Executive Director

cc: Nancy K. Kopp, Chair of the Board of Trustees
Ira Greenstein, Chief Information Systems Officer
David Rongione, Chief Internal Auditor

Maryland State Retirement Agency
Response to Legislative Fiscal Compliance Report

Referring to pages 5-6 of your draft "Findings and Recommendations", the audit finding and recommendations along with the Agency response are as follows:

Finding 1

The Agency's procedures for reviewing certain critical security events were not sufficient.

Recommendation 1:
We recommend that the Agency:

a. review critical MPAS database and server security events, audit events, and direct modifications to critical tables;
b. document these reviews; and
c. retain the documentation for future reference.

Agency Response
SRA agrees with this finding.

a. The Agency has already implemented a process to ensure more timely review of critical MPAS database and server security events, audit events, and direct modifications to critical tables. A software product had previously been in production to perform this function; however, this product created technical conflicts with other installed products and had to be partially disabled (including the time period when auditors were on-site). A replacement software product was selected and implemented in November 2014. The replacement software is functioning properly.
b. The Agency will properly document these reviews.
c. The Agency will retain the documentation for future reference.

Finding 2

The Agency's intrusion detection prevention system was not properly protecting the network.

Recommendation 2:

We recommend that the Agency perform a documented review and assessment of its network security risks and identify how IDPS coverage should be best applied to its network and inbound encrypted traffic. Based on this review and assessment, we recommend that the Agency implement IDPS coverage as necessary.

Agency Response

SRA agrees with this finding. The Agency will perform an assessment of its network security risks by 6/30/2015, focusing on the security and operational impacts of extending IDPS coverage, and document the results. Then, based on a risk analysis of the results, the Agency will implement IDPS coverage as necessary by 12/31/2015.

AUDIT TEAM

Mark S. Hagenbuch, CPA
Audit Manager

Richard L. Carter, CISA
Stephen P. Jersey, CPA, CISA
Information Sytems Audit Managers

Menachem Katz, CPA
Senior Auditor

Eric Alexander, CPA
Michael K. Bliss, CISA
Information Systems Senior Auditors

Samuel Hur
Lauren E. McLain, CPA
Staff Auditors

Edward O. Kendall
Information Systems Staff Auditor