THE AUDIT COMMITTEE
of the
BOARD OF TRUSTEES
MARYLAND STATE RETIREMENT AND PENSION SYSTEM

MINUTES OF THE MEETING OF April 20, 2021

The Audit Committee convened on Tuesday April 20, 2021 at 11:30 a.m. via video conference call with the host site at 120 East Baltimore Street, Baltimore, Maryland.

Committee members present were: David Hamilton, Chairman
    Richard E. Norman, Vice-Chairman
    Thomas M. Brandt
    Kenneth B. Haines
    James P. Daly, Jr.

MSRA attendees were: R. Dean Kenderdine, Executive Director
    Kenneth Reott, Retirement Administrator
    Kimberly O'Keefe, Retirement Administrator
    David Rongione, Chief Internal Auditor
    Rachel Cohen, Principal Counsel
    Toni Voglino, Senior Compliance Officer
    Ira Greenstein, Chief Information Systems Officer
    Robert Diehl, Deputy Chief Information Systems Officer
    Melody Countess, Chief Operating Officer
    Patricia Fitzhugh, Deputy Chief Operating Officer
    Lauren Smith, Internal Audit Contract Manager
    Gregory Busch, IT Audit Manager
    Richa Sultana, Internal Audit Supervisor

BD&Co. attendees were: Jeff Binford, Engagement Partner

    A. Minutes of the January 19, 2021 Audit Committee Meeting
    On a motion made by Mr. Norman and seconded by Mr. Daly, the minutes of the January 19, 2021 Audit Committee meeting were approved.

    B. Investment Operations – Accounting Audit Report – Results presented by BD&Co
    Mr. Rongione directed the Committee to the final audit report for the Investment Operations Accounting Audit. Mr. Rongione advised that the report is rated 'Yellow' meaning improvement is needed in the area of control and compliance. Management generally agreed with all findings. The Committee had no questions on the final report.

    C. Agency Wide Risk Assessment
    Mr. Rongione advised that the annual risk assessment will begin in the next few weeks. This includes sending a questionnaire to AC members, Executive staff, Unit directors, as well as

interviews of select staff. Internal audit will utilize the results of these interviews and questionnaires to evaluate risks based on likelihood and impact. The results of the risk assessment will be factored into the FY 22 audit plan, which will be presented at the next meeting.

Mr. Hamilton inquired about PGU repeat offenders in relation to the past due balances owed to the Agency. Chief Operating Officer, Melody Countess and Executive Director Dean Kenderdine advised that they spoke to the Comptroller's Office regarding offsets. Currently, offsets can occur for past due Administrative fees and past due Annual Billing fees. There currently is no provision to offset the past due automatic enrollment fees. The current plan is to send more frequent past due letters from the Executive Director. Mr. Hamilton requested a recommendation from staff at the next Audit Committee meeting whether the Agency should pursue legislation for offsetting past due automatic enrollment fees.

D. **Audit Plan Status**
Mr. Rongione directed the Committee to the FY21 Audit Plan Status. The Network Security Audit covering the third and fourth quarters of FY20 is complete. The exit meeting was held last week for the General Controls Audit covering the fourth quarter of FY20 and the first quarter of FY21; a report will be issued in the coming weeks. Five of the eight PGU audits conducted internally are complete with the remaining three in the fieldwork phase. The outsourced Investment Contractual Risk Audit has kicked off and is in progress. Participating employer audits conducted externally are 10% complete, 10% complete pending management response, 70% in progress and 11% of audits not started. Except for the Cybersecurity Audit, Mr. Rongione advised that all audits are expected to be completed by the end of fiscal year. The RFP for the Cybersecurity Audit is expected to be released shortly.

E. **Data Analytic/Continuous Audit Dashboard**
Mr. Rongione directed the Committee to the continuous audit dashboard. The dashboard includes the number of exceptions per month for the applicable audit. Two additional graphs were provided; one graph shows the number of exceptions relative to the samples audited and the other shows the number of remediated findings compared to the number of exceptions. Page two of the dashboard explains the audits.

F. **Open Issues Log**
Mr. Rongione presented the listing of open issues noting that Internal Audit was able to close out eight issues since the last meeting; ten issues were added with completion of the most recent audits.

As a follow-up to the last meeting regarding the SOC2 open issues, Mr. Rongione spoke with Trustee Brandt to review the Agency's current procedures and also spoke to Executive Director, Mr. Kenderdine, on enhancements to the current procedures with the staff responsible for reviewing the SOC2 reports. Enhancements to the current procedures include having procurement maintain a listing of vendors that have a SOC2 requirement in the contract. New vendors will be added to the listing as they come on board. All contract monitors have reached out to current vendors to obtain the latest SOC2 reports. If not available, they inquire when the next report will be issued. The contract monitor maintains an annual calendar appointment to remind them of the request to obtain the SOC2 report annually. In addition to the contract monitor, Ms. Janet Sirkis from the Executive Director's Office, will maintain a calendar with all SOC2 report dates in case any turnover with the contract monitors.

Mr. Brandt advised that the SOC2 reports are difficult and dense documents and figuring out a way to escalate topics of significance with the Audit Committee becomes a communication challenge.

Mr. Daly believes some educational work needs to be done around this for the trustees.

Mr. Rongione gave background on Agency SOC2 procedures. With each vendor and applicable contract there is a contract monitor assigned. That contract monitor manages that contract including billing and any customer relation issues. The contract monitor reaches out to the vendor annually for their SOC2 report. When the report is received there is a review template to determine that independent audit report issued for the SOC2 has an unqualified opinion. The contract monitor also reviews control testing to verify if there were any exceptions and if an appropriate response to the exceptions were given. A write-up is prepared to tell if we are comfortable with the report. The next step is to look at the user entity control considerations. This section details what the vendor is saying the internal controls the vendor believes the Agency should have in place. The contract monitor will document Agency controls in place and send over to Information Systems to provide input as well. Lastly, a sign off is done when the review is completed.

Mr. Daly inquired about how a breach would be communicated in a SOC2 report. Mr. Rongione advised that SOC2 type II reports on the internal control environment and would list any exceptions identified during testing. Mr. Rongione further advised that Agency contracts require the vendor to immediately inform the Agency of a cybersecurity incident.

In addition to educating Trustees, Mr. Daly questioned how we are ensuring participants that their information is indeed secured and what response do we have for a breach.

Mr. Brandt added that due to the dynamic environment of cybersecurity, communications cannot be ritualized because exposures are constantly changing. We must come up with a systemic execution of our responsibilities and a record of it. Mr. Brandt added that it is a high challenge to figure out how to talk to the Audit Committee in a way that all can understand and keep up with.

Chief Information Systems Officer, Ira Greenstein, advised that the standard in Agency contracts include providing notification to the Agency of any breaches and/or exposure to sensitive data. Second, the Agency takes a stringent view on data, by treating all data as sensitive. The Agency encrypts all data so if there is a breach the offender(s) will find data encrypted and unreadable. The encryption is done at hardware level. Data is stored on a piece of hardware backed up to the site in Annapolis and that too is encrypted on a hardware level; even something as simple as a memo is encrypted. Lastly, the Chief Information Systems Officer will provide a briefing that will be delivered to the Board of Trustees in June. The briefing list explanations on how our approach to cybersecurity is protecting our resources.

Mr. Greenstein advised that the Agency has gone through a multiyear process to get additional IT security positions approved for the Agency. Mr. Greenstein praised the Board and Executive Staff of the Agency for supporting this area of cybersecurity. We have the tools we need to be able to protect our Agency; those tools will be covered in the June briefing by Mr. Greenstein.

G. Other Business
The External Quality Assurance Review has been kicked off. The review is required every three years, and it ensures the Internal Audit Division is operating within auditing standards. The external auditor conducting the review will be reaching out to committee members to obtain input. As mentioned earlier, the Cybersecurity procurement is close to being issued. The next legislative audit by OLA will be kicking off shortly. There is a kickoff meeting scheduled for tomorrow, April 21, 2021.

H. Motion by the Audit Committee to meet in Closed Session
On a motion made by Mr. Norman and seconded by Mr. Daly the Audit Committee met in closed session.

I. Motion to Adjourn
On a motion by Mr. Norman and seconded by Mr. Brandt, the Committee approved to adjourn the meeting at 12:20 p.m.

Respectfully submitted,

_____

David Rongione, Secretary