

**MINUTES OF THE
WV CONSOLIDATED PUBLIC RETIREMENT BOARD
INTERNAL AUDIT COMMITTEE MEETING
OF OCTOBER 2, 2018**

A meeting of the West Virginia Consolidated Public Retirement Board (CPRB) Internal Audit Committee was held in the Legal Conference Room located at the offices of the CPRB, 4101 MacCorkle Avenue, SE, Charleston, West Virginia, on Tuesday, October 2, 2018. The meeting was called to order at 1:00 p.m. by Deputy Cabinet Secretary, Mary Jane Pickens, Chair.

Roll Call

Members present were:

Deputy Cabinet Secretary Mary Jane Pickens, Chairman
Diana Stout
Jeff Waybright, *via conference call*
Captain Michael Corsaro
Jeff Vallet

A quorum was present.

Due notice had been published.

Also, present were:

Jeffrey Fleck, CPRB Executive Director
Terasa Miller, CPRB Deputy Director
Nancy Butcher, Executive Assistant
Tina Baker, CPRB Internal Auditor
Tim Abraham, CPRB Compliance Officer
Lisa Trump, Manager, Retirement
Tammy White, Assistant Manager, Retirement

Item #1: Approval of the July 17, 2018, Meeting Minutes.

Captain Corsaro made a motion to approve the July 17, 2018 meeting minutes. The motion was seconded by Ms. Stout. The motion carried.

Item #2: Review of Retiree Self Service Portal.

Ms. Baker reviewed the Internal Audit of the Retiree Self Service portal. She explained that the objective of the audit was to review the controls in place to prevent fraudulent account

access in the Retiree Self Service (RSS) portal. The scope of the review included controls implemented as part of the RSS.

Summary of Findings

1. Given that there is limited sensitive data available in RSS and little information able to be changed or updated on the system, incorporating more stringent controls would likely cause unnecessary delays, costs, or complications. However, if in the future other risks come to light or it is decided to offer additional information or services in RSS, controls should be enhanced accordingly.

CPRB Retiree Self-Service Portal Controls

Incidents of account takeovers have occurred with self-service portals administered by several other public pension systems, including the Iowa Public Employees' Retirement System (IPERS), the New York State Teachers' Retirement System (NYSTRS), the Public School Retirement System of Missouri (PSRSMO), and the Ohio Public Employees Retirement System (OPERS). As a result, the Association of Public Pension Fund Auditors has held panels on the topic of self-service portal controls and provided the document in Appendix A detailing control options, the strength of the control activities, and the pros and cons of each. Table 1 illustrates which of these controls is present in RSS.

Table 1 RSS Controls	
Control	RSS
Monitor IP Risk Rating	X
Geo-blocking	X
Geo-fencing	X
Sensitive data masking	Social security numbers are truncated, displaying the last four digits only. Birthdates are not masked. No bank account information is maintained in RSS.
Waiting period	X
Negative confirmation of account opening	If the individual provides an email address, a negative

	confirmation email is sent. If no email is provided, a negative confirmation is not mailed to the mailing address on file.
Positive confirmation of account opening with security code	X
Challenge questions using retirement system database	After entering the user name and password, the individual is asked to answer a challenge question, such as the last four digits of his/her social security number or the zip code on file.
Challenge questions using public records	X
Use of member number for registration instead of social security number	X
Password strength requirements	Passwords must be 8-16 characters and contain at least one capital letter, one number, and one special character.
Account lockout after multiple failed log-in attempts	✓
Account logout after a period of inactivity	✓
Multi-factor authentication – PIN sent to email	X
Multi-factor authentication – PIN sent to phone	X
Negative confirmation of transaction to postal address	The only transaction that generates a negative confirmation mailing is the change of address. If tax information is changed, the member will receive a Change Letter when the next payroll is run. If an email address has been provided, negative confirmation is emailed for some transactions, such as registration, change in User ID or password, or update in contact information.
Positive confirmation of transaction with security code to postal address	X
Personal challenge questions when effecting a transaction	X
Prior information challenge questions when effecting a transaction	X
User imposed restriction on account functionality	X
Deactivate dormant accounts	X
Provide a landing page that states the time and date of last login	A bar at the top of each page provides the last login date and time.

Most incidents of account takeovers in other states have involved direct deposit information. During the planning phase for RSS, risks were assessed, and decisions were made as to what functions to make available to retirees. It was decided not to allow changes to potentially risky

information such as direct deposit information. The information and transactions that are available in RSS include:

- Account summary – displays retirement option, monthly benefit amount, and beneficiary information.
- Payment history – displays payment details, such as the monthly benefit amount and deductions.
- Invoices – displays current and previous invoices for overpayments.
- Tax information – displays 1099-R and withholding information and allows changes to tax withholding.
- Contact information – displays and allows changes to contact information, such as mailing address, phone number, email address, and User ID and password.
- Correspondence – displays a list of sent and received correspondence.
- Income Verification Letter – allows a request for retirement income verification letter to be submitted online.

As shown in Table 1, there are some control functions that are not included or could be enhanced in RSS. However, it is important to balance safety with customer service. Given that there is limited sensitive data available in RSS and little information able to be changed or updated on the system, incorporating more stringent controls would likely cause unnecessary delays, costs, or complications. However, if in the future other risks come to light or it is decided to offer additional information or services in RSS, controls should be enhanced accordingly. **It is recommended that periodic risk assessments be conducted to provide assurance that RSS controls are adequate to prevent account takeovers or other fraudulent activities.**

Recommendations

- 1. It is recommended that periodic risk assessments be conducted to provide assurance that RSS controls are adequate to prevent account takeovers or other fraudulent activities.**

There was discussion regarding security measures and concerns with breaches of the security systems. Ms. Stout moved to accept the report of the Internal Auditor. Mr. Waybright seconded the motion. The motion carried.

Item #3: Updated 2018 Internal Audit Plan.

Ms. Baker gave an update of the 2018 Internal Audit Plan and answered questions from the committee members regarding the plan.

Item #4: Tentative 2019 Internal Audit Plan.

Ms. Baker explained the tentative 2019 Internal Audit Plan. There was discussion about the Internal Audit Plan and issues with OASIS. Captain Corsaro suggested that the Internal Auditor look at some of the issues with OASIS. Mr. Vallet made a motion to accept the 2019 Internal Audit Plan. Ms. Stout seconded the motion. Ms. Stout moved to amend the motion to include the issues of the data and information exchange from OASIS to COMPASS. Mr. Vallet seconded the motion to amend the motion. The motion to amend carried. The motion to accept the 2019 Internal Audit Plan, as amended, carried.

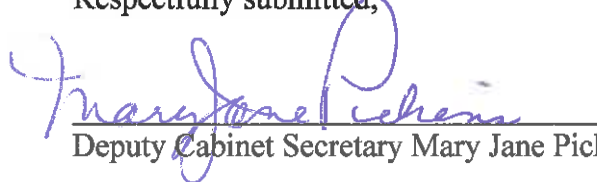
Item #5: Wood County Board of Education Report.

Ms. Baker presented the *Independent Accountant's Report in Applying Agreed-Upon Procedures* report from the State Auditor on the Wood County Board of Education's participation in the applicable state-wide retirement systems and associated findings. She discussed the findings. Ms. Baker, Ms. Miller, Mr. Waybright and Tammy White, Assistant Manager of the

Retirement Section, responded to questions from the committee members. The report was received.

There being no further business to come before the committee, Captain Corsaro made a motion to adjourn the October 2, 2108, meeting of the CPRB Internal Audit Committee. The motion was seconded by Mr. Vallet. The motion carried.

Respectfully submitted,


Deputy Cabinet Secretary Mary Jane Pickens, Chair


Jeffrey E. Fleck, Executive Director