



Audit and Compliance Committee Meeting

[1111 E. Main Street](#)
[Third Floor Board Room](#)

Thursday, 6/16/2022

2:00 - 4:00 PM ET

- I. Welcome
- II. Minutes of the March 29, 2022 Meeting
 - Meeting Minutes - Page 2*
- III. Matters for Discussion with the Auditor of Public Accounts
 - Matters for Discussion with the APA - Page 6*
 - 03b - 2021 APA EA Board Update and ACFR Entrance - Page 7*
 - A. Update on the 2021 Employer Assurances Review
 - B. Entrance on 2022 Annual Comprehensive Financial Report
- IV. Audit Reports
 - A. Report 443: Cash Management
 - Audit Report - Cash Management - Page 38*
 - B. Report 444: Review of IT General Controls
 - Audit Report - General Controls - Page 66*
 - Management's Response - Page 102*
- V. Miscellaneous Updates
 - A. Quarterly Report on Fraud, Waste and Abuse Hotline Cases
 - Fraud Waste and Abuse Report - February 1 through April 30 2022 - Page 110*
 - B. Management's Quarterly Travel Expenses and Per Diem Report
 - Quarterly Travel Expense Report_Period Ending 03_31_22 - Page 113*
 - C. Next Meeting Date: Tuesday, September 13, 2022 at 2:00 p.m.

Minutes

The Audit and Compliance Committee of the Board of Trustees met on March 29, 2022, at the Virginia Retirement System located in Richmond, Virginia. The following individuals were present.

Audit and Compliance Committee Members:

Joseph W. Montgomery, Committee Chair
W. Brett Hayes, Committee Vice Chair
O’Kelly E. McWilliams, III, Board Chair

Other Members of the Board of Trustees:

John M. Bennett
Troilen G. Seward, Ed.S.

VRS Staff:

Patricia Bishop, Jennifer Schreck, Judy Bolt, Richard Brooks, Jeanne Chenault, Michael Cooper, Valerie Disanto, Barry Faison, Laurie Fennell, Joshua Fox, John T. Grier, Krystal Groff, Robert Irving, Chung Ma, Matthew Priestas, Mark Rein, and Kristy Scott.

Guests:

Jamie Bitz, Department of Planning and Budget; and Brian Deveney, Auditor of Public Accounts

The meeting convened at 2:00 p.m.

Opening Remarks

Joseph W. Montgomery called the meeting to order and welcomed everyone to the March 29, 2022 meeting of the Audit and Compliance Committee of the Virginia Retirement System Board of Trustees and noted no changes or additions to the meeting agenda.

Approval of Minutes

Upon motion of Mr. McWilliams, seconded by Mr. Hayes, the Committee approved the minutes of the Audit and Compliance Committee meeting held on December 6, 2021.

Audit Report

The Committee received one audit report from staff.

Audit Report 442

Mr. Fox presented audit report 442 – Conformance with VITA’s Security Program. The review determined as of the audit period that VRS’ security policies and standards are partially compliant with VITA’s Information Technology Security Program, with updates to VRS’ policies and standards currently underway. The Committee discussed the timing of recent changes to VITA requirements relative to when the review was performed, and VRS’ process for updating its policies and standards. There were no written recommendations resulting from the review.

Acceptance of the Audit Report

Upon motion of Mr. McWilliams, seconded by Mr. Bennett, the Committee accepted audit report 442 as presented.

Annual Report on Code of Ethics

Ms. Schreck discussed the Internal Audit department's adherence to the VRS Code of Ethics and Institute of Internal Auditors' Code of Ethics. She noted members of Internal Audit also hold various other professional designations and memberships, which provide similar frameworks for ethical behavior in the practice of that profession. Members of the Internal Audit staff complete annual certifications required by these professional organizations.

Mr. Cooper provided a brief overview of VRS' Code of Ethics and the training provided to personnel. Mr. Cooper confirmed all eligible VRS staff had completed the annual code of ethics training by December 31, 2021.

Mr. Brooks discussed the Investment Department's Code of Ethics and Standards of Professional Conduct Policy and compliance monitoring, noting all Investment associates were in compliance as of December 31, 2021.

Audit Plan Progress as of December 31, 2021

Ms. Schreck reported on the progress of the annual Audit Plan as of December 31, 2021, the mid-point of the fiscal year. She noted Internal Audit is on track to complete the annual Audit Plan as approved.

Miscellaneous Updates

Quarterly Report on Fraud, Waste and Abuse Hotline Cases

Ms. Schreck noted there were no Fraud, Waste and Abuse cases reported for the period November 1, 2021 through January 31, 2022.

Internal Audit's Review of the Cost-of-Living Adjustments

Ms. Schreck informed the Committee that Internal Audit has reviewed the amounts referred to as "Cost-of-Living Adjustments (COLA)" as calculated by VRS' actuary, Cavanaugh Macdonald Consulting, LLC, to be effective July 1, 2022. Ms. Schreck noted Internal Audit independently recalculated the "Cost-of-Living Adjustments" and found them to be valid and accurate. The results of this review were provided to the Benefits and Actuarial Committee and Board of Trustees in February 2022 to support their review and approval process for these adjustments. The Committee discussed Internal Audit's process of reviewing the COLA.

Management's Quarterly Travel Expense and Per Diem Report

Ms. Schreck noted management's quarterly travel expense and per diem report was included in the meeting materials for the Audit and Compliance Committee's review.

Next Committee Meeting Date

Ms. Schreck noted the next meeting of the Committee is scheduled for June 16, 2022, at 2:00 p.m.

Meeting Adjournment

There being no further business, upon motion by Mr. McWilliams, seconded by Mr. Hayes, the Audit and Compliance Committee agreed to adjourn the meeting at approximately 2:21 p.m.

Committee Chair

Secretary

Matters for Discussion with the Auditor of Public Accounts

VRS Annual Report

For informational purposes, you may wish to review VRS' most recent Annual Report, which includes VRS' 2021 Annual Comprehensive Financial Report and the APA's associated opinion. Due to the voluminous nature, the report is not included in the meeting book, but can be found on VRS' website at the following link:

<https://www.varetire.org/pdf/publications/2021-annual-report.pdf>

APA's Report on Internal Control

The APA's Report on Internal Control for the 2021 Annual Report Audit found the financial statements were presented fairly, in all material respects; no internal control findings requiring management's attention; and, no instances of noncompliance or other matters required to be reported under Government Auditing Standards. This report can be viewed at the following link:

<https://apa.virginia.gov/reports/VirginiaRetirementSystem2021.pdf>

MATTERS FOR DISCUSSION WITH THE APA

Update on the 2021 Employer Assurances Audit

The APA will provide an update on the status of their 2021 Employer Assurances Audit, the results of which are expected to be reported out by the end of July 2022.

Entrance on VRS' 2022 Financial Statement Audit

The APA will entrance with the Committee on VRS' 2022 Annual Comprehensive Financial Report Audit.

For reference purposes, a list of some of the questions often posed to external auditors when entrancing are provided below. However, entrance meetings with the APA are typically informal, with questions posed as the Committee sees fit.

Typical Questions Posed to External Auditors When Entrancing:

- Do you anticipate any substantial changes in your audit approach, scope, standards, procedures, resources allocated, or other circumstances, which may significantly affect your examination?
- Are there any significant changes in generally accepted accounting principles or other changes which will significantly impact your examination, our financial reporting or your opinion thereon?
- Have you identified any possible changes in the character of VRS' activities? Have these changes, if any, affected your audit approach or scope?
- Are there any special areas in which you expect to focus?
- Are there any potential restrictions on your audit scope or other matters that could affect your audit opinion?
- Do you foresee any significant problems and, if so, how will they be handled?
- Are there any issues the Committee needs to be aware of or are there any areas where you require special assistance or cooperation from VRS?



2021 VRS Employer Assurances Engagement

June 16, 2022

Zach Borgerding, Audit Director

Auditor of Public Accounts

Pension and OPEB Plan Types

Single Employer

- Single plan that covers the employees of a single employer

Agent Multiple Employer

- Single plan that covers the employees of multiple employers
- Plan assets are segregated for each participating employer and cannot legally be used to pay other employer's pension or OPEB obligation

Cost Sharing Multiple Employer

- Single plan that covers the employees of multiple employers
- Plan assets are not legally segregated for each participating employer and can legally be used to pay other employer's pension or OPEB obligation

Agent Multiple Employer Plans

- Pensions – Political Subdivisions



- Health Insurance Credit – Political Subdivisions



Agent Multiple Employer Plan Audit Assurances

Provide opinion on proper accumulation of census data by the plan

Provide opinion on fair presentation of changes in FNP by employer

Net Liability is the Residual Balance

Total Pension Liability

Less: Fiduciary Net Position

Net Pension Liability

Total OPEB Liability

Less: Fiduciary Net Position

Net OPEB Liability

VRS Cost Sharing Multiple Employer Plans

PENSION

- State Plan
- Teacher Plan

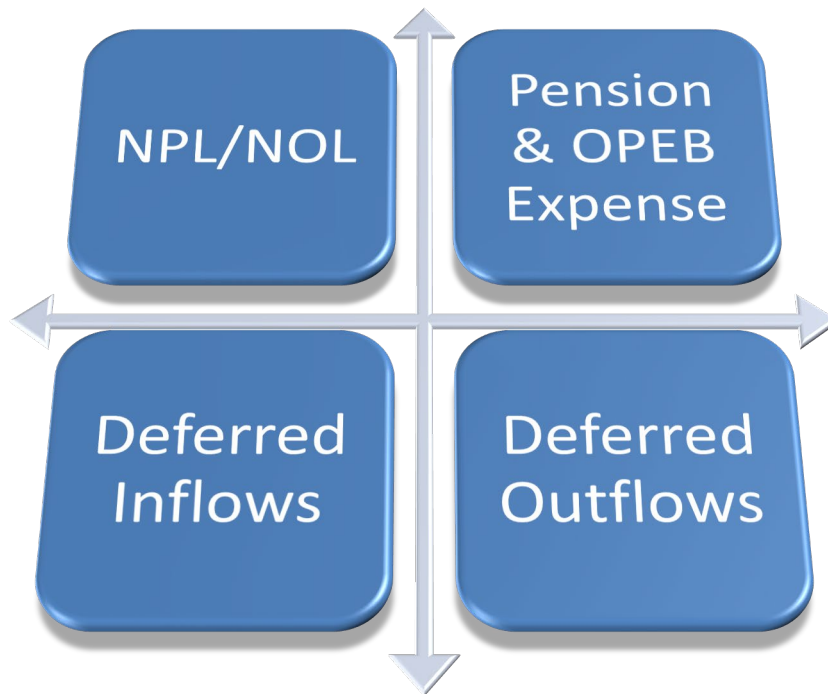
OPEB

- Health Insurance Credit – Teacher
- Health Insurance Credit – State
- Group Life Insurance
- Line of Duty Act
- Virginia State Disability Program
- Virginia Local Disability Program (No opinions)

Cost Sharing Multiple Employer Audit Assurances

- Provide opinion on pension/OPEB amounts at plan level

- Provide opinion on employer allocation percentages



Employer Code	Employer	Employer Contributions	Employer Allocation Percentage
40100	ACCOMACK COUNTY SCHOOL BOARD	\$ 3,023,764	0.35461%
40101	ALBEMARLE COUNTY SCHOOLS	9,491,479	1.11311%
40102	ALLEGHANY COUNTY SCHOOL BOARD	1,435,188	0.16831%
40103	AMELIA COUNTY SCHOOL BOARD	903,338	0.10594%
40104	AMHERST COUNTY SCHOOL BOARD	2,704,879	0.31721%
40105	APPOMATTOX COUNTY SCHOOL BOARD	1,176,909	0.13802%
40106	ARLINGTON PUBLIC SCHOOLS	29,095,514	3.41217%
40107	AUGUSTA COUNTY SCHOOL BOARD	6,291,642	0.73785%
40108	BATH COUNTY SCHOOL BOARD	498,809	0.05850%
40109	BEDFORD COUNTY SCHOOL BOARD	5,682,514	0.66642%
40110	BLAND COUNTY SCHOOL BOARD	483,108	0.05666%
40111	BOTETOURT COUNTY SCHOOLS	3,106,162	0.36427%
40112	BRUNSWICK COUNTY PUBLIC SCHOOLS	1,137,210	0.13337%
40113	BUCHANAN COUNTY SCHOOL BOARD	1,757,633	0.20613%
40114	BUCKINGHAM COUNTY SCHOOL BOARD	1,213,826	0.14235%

APA Expects to Issue Unmodified Opinions for:

- Accurate and complete accumulation of census data to the actuary for pensions and OPEBs
- Fair presentation of the Schedules of Changes in Fiduciary Net Position at the employer level and related notes
- Fair presentation of pension/OPEB amounts and employer allocations and related notes

We project dating reports as early as June 22nd and issuing reports in July

Census Data Opinion: Emphasis of Matter

- VRS does not have access to certain census data elements for retirees from an Optional Retirement Plan (ORP) who are eligible for HIC or GLI and have not claimed a benefit
- Actuary has applied assumptions in place of the data in accordance with Actuarial Standards of Practice
- Opinion was not modified in respect to this matter

Other Audit Results:

- No internal control weaknesses that we would consider significant deficiencies or material weaknesses
- No indications of non-compliance, fraudulent activity or illegal acts
- Proper treatment of accounting principles
- No material alternative accounting treatments
- No significant disagreements with management
- Material adjustments made to 4 out of 854 multiple agent plans (<\$300,000 in aggregate)

Issuance of GASB 68 and 75 Resources

- Employers will receive pension and OPEB resources, including the following:

Audited Schedules



GASB 68/75 Reports

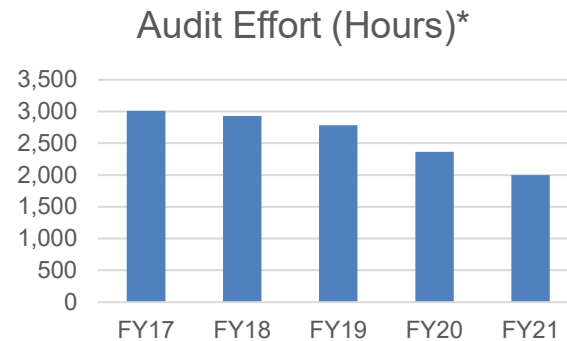
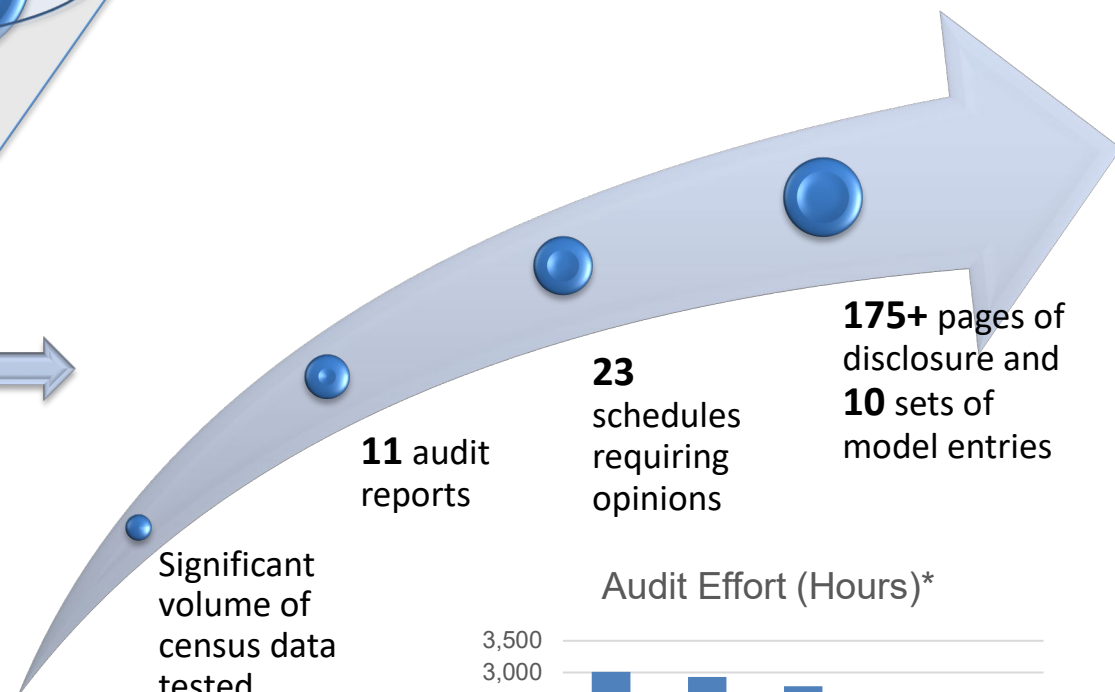
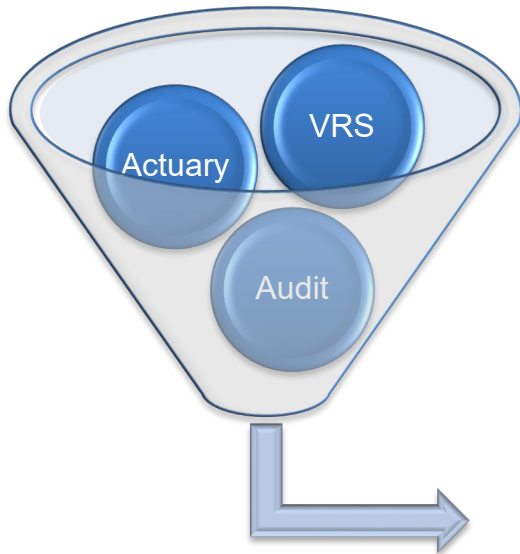


Template Journal Entries



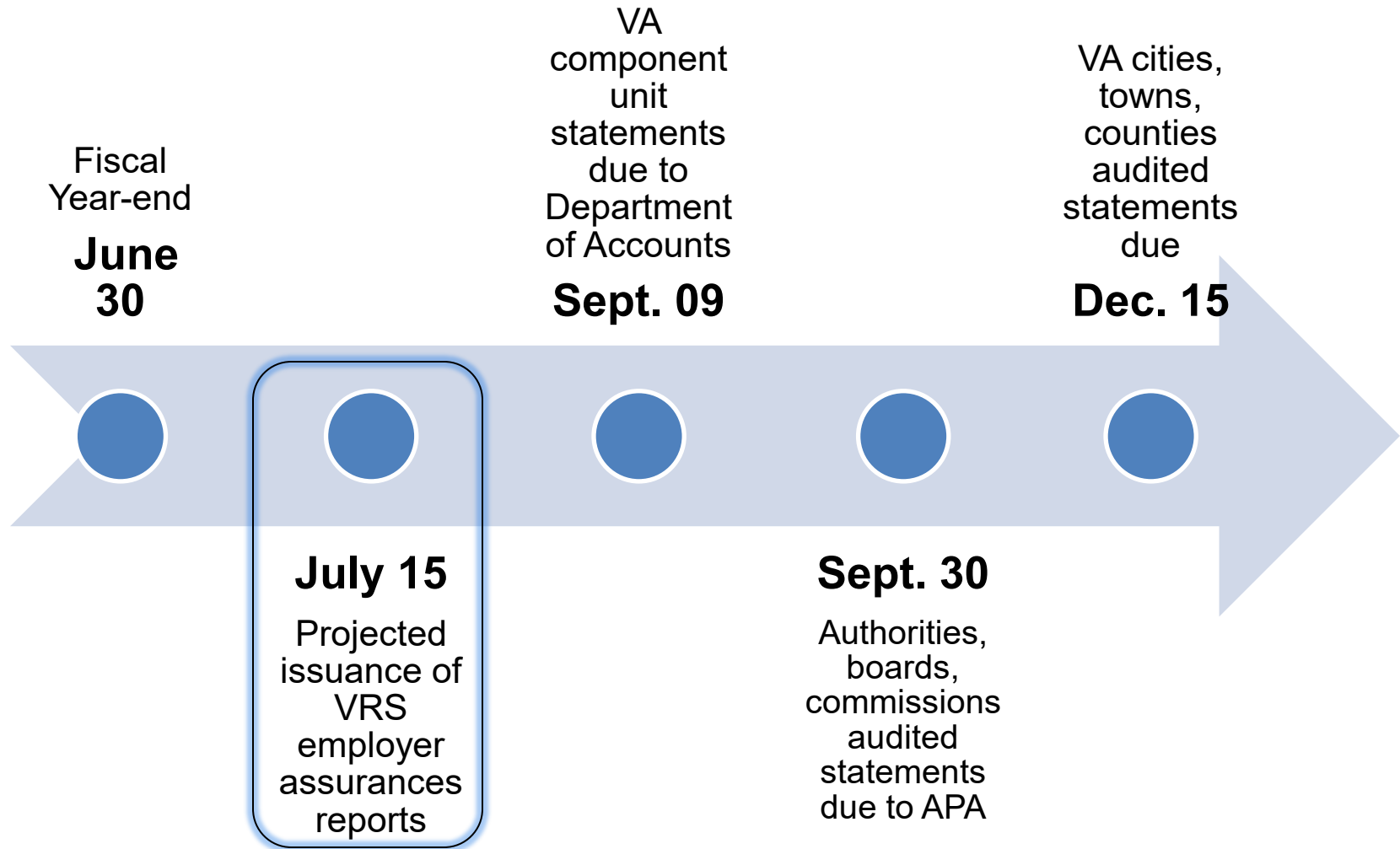
Template Note Disclosures

GASB 68 and 75 Project Scope



* FY21 projected based on current progress.

Timely Issuance Projected for Employers



Employer Auditor Communications

- VRS audit team annually updates *Specifications for Audits of Counties, Cities, and Towns* and *Specifications for Audits of Authorities, Boards and Commissions* for GASB 68 and 75 requirements
- Local auditors must test active employee data and submit results to APA
- APA Local Government Audit Manager and the VRS audit team communicate with local employer auditors to address inquiries

VRS Annual Comprehensive Financial Report

AUDIT ENGAGEMENT ENTRANCE

Audit Logistics

- Timing:
 - Audit Period: July 1, 2021 – June 30, 2022
 - Audit Timing: June, 2022 – December, 2022
 - Must have sufficient, appropriate audit evidence by December 15th
- Audit Team:
 - Several audit team members are returning from the prior year
 - Continued use of co-in-charge model

Our Team

Zach Borgerding

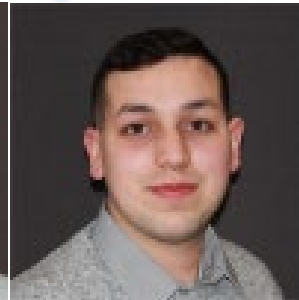
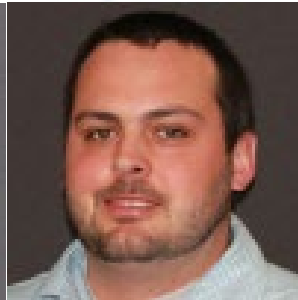
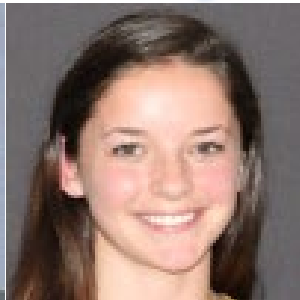
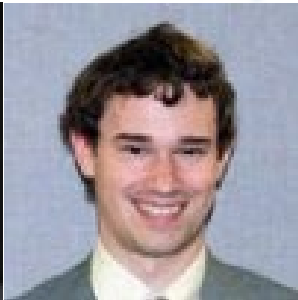
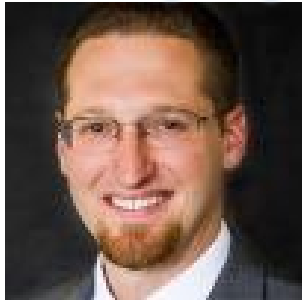
Brian Deveney

Erin Rodriguez

Gary Gammon

Igor DeOliveira

Ben Rupert



- Director
- 14 years experience
- 7 years experience with VRS
- CPA, CISA and CGFM
- Specialty Focus: Reporting and Standards

- Supervisor
- 9 years experience
- 4 years experience with VRS
- CPA, CISA, and Masters of Accountancy
- Specialty Focus: Reporting and Standards

- Senior
- 4 years experience
- 4 years experience with VRS
- MBA
- Specialty Focus: Data Analysis

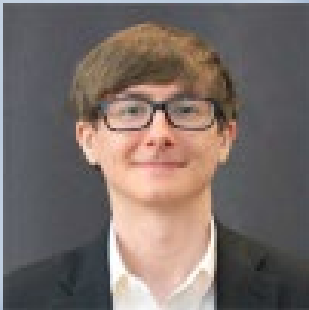
- Supervisor
- 5 years experience
- 1st year assigned to VRS
- CFE
- Specialty Focus: Strategic Risk and Project Management

- Auditor
- 1.5 years experience
- 3 months experience with VRS
- Passed CPA exam
- Specialty Focus: Compliance Assurance

- Associate Auditor
- 1 year experience
- 1st year assigned to VRS
- Specialty Focus: Data Analysis

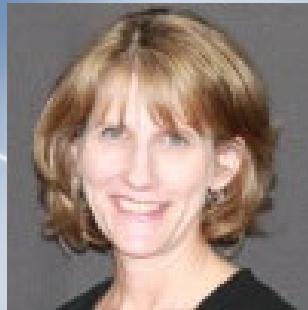
Our Team (continued)

Taylor Collins



- Auditor
- 1.5 years experience
- 1 year assigned to VRS
- BS in Information Systems
- Assigned exclusively to audit systems security

Danese Seabourne



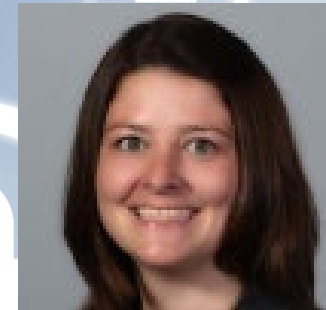
- Manager
- 7 years experience
- 6 years assigned to VRS
- BS in Computer Science and certified in info systems, CISA
- Assigned exclusively to audit systems security

Goran Gusavsson



- Director
- 26 years experience
- BS in Electrical Engineering and Computer Science, MA in ISS, CISM, and CISSP
- Manages and reviews all ISS audits

April Cassada



- Director
- 19 years experience
- BS in Accounting, CPA, CISA, and CITP
- Manages and reviews all data retrieval work

Audit Objectives

- **Basic Financial Statements**
 - Primary objective of audit is to provide an opinion on fair presentation in accordance with GAAP
 - We assess risk of material misstatement at the line item level and design an audit approach responsive to those risks
 - Procedures include a combination of tests of detailed transactions and balances, as well as internal control processes

1. INTRODUCTORY SECTION		
Chair's Letter	9	Schedule of Employers' Net OPEB Liability by Program and Plan 87
Board of Trustees	14	Schedule of Actuarial Methods and Significant Assumptions: OPEB Plans 88
VRS Organization	15	Schedule of Impact of Changes in Discount Rate: LODA Plan 89
Investment Advisory Committee	15	Schedule of Impact of Changes in Health Care Trend Rate: LODA Plan 89
Defined Contribution Plans Advisory Committee	15	Schedule of Impact of Changes in Discount Rate: Non-LODA OPEB Plans 90
Executive Administrative Team	16	Required Supplementary Schedule of Changes in Employers' Net Pension Liability: VRS State 116
Executive Investment Team	16	Required Supplementary Schedule of Changes in Employers' Net Pension Liability: VRS Teacher 118
Professional Consultants	16	Required Supplementary Schedule of Changes in Employers' Net Pension Liability: VRS Political Subdivisions 120
Letter of Transmittal	17	Required Supplementary Schedule of Changes in Employers' Net Pension Liability: SPORS 122
2. FINANCIAL SECTION		Required Supplementary Schedule of Changes in Employers' Net Pension Liability: VaLORS 124
Independent Auditor's Report	31	Required Supplementary Schedule of Changes in Employers' Net Pension Liability: JRS 126
Management's Discussion and Analysis	35	Required Supplementary Schedule of Employer Contributions: Pension Plans 128
Basic Financial Statements:	46	Required Supplementary Schedule of Investment Returns 129
VRS Statement of Fiduciary Net Position: Defined Benefit Pension Trust Funds and Other Employee Benefit Trust Funds	46	Required Supplementary Schedule of Changes in Employers' Net OPEB Liability and Related Ratios 130
VRS Statement of Changes in Fiduciary Net Position: Defined Benefit Pension Trust Funds and Other Employee Benefit Trust Funds	47	Required Supplementary Schedule of Employer Contributions: OPEB Plans 141
VRS Statement of Fiduciary Net Position: Defined Benefit Pension Trust Funds	48	Schedule of Investment Expenses 144
VRS Statement of Changes in Fiduciary Net Position: Defined Benefit Pension Trust Funds	49	Schedule of Administrative Expenses 145
VRS Combining Statement of Fiduciary Net Position	50	Schedule of Professional and Consulting Services 146
VRS Combining Statement of Changes in Fiduciary Net Position	51	3. INVESTMENT SECTION
VRS Combining Statement of Fiduciary Net Position: Other Employee Benefit Trust Funds	52	Chief Investment Officer's Letter 149
VRS Combining Statement of Changes in Fiduciary Net Position: Other Employee Benefit Trust Funds	53	Investment Account 153
Retiree Health Insurance Credit Combining Statement of Fiduciary Net Position	54	Portfolio Highlights 155
Retiree Health Insurance Credit Combining Statement of Changes in Fiduciary Net Position	55	VRS Money Managers 161
VLDP Combining Statement of Fiduciary Net Position	56	Public Equity Commissions 164
VLDP Combining Statement of Changes in Fiduciary Net Position	57	Schedule of Investment Expenses 164
VRS Statement of Fiduciary Net Position: Other Custodial Plans	58	Investment Summary 165
VRS Statement of Changes in Fiduciary Net Position: Other Custodial Plans	58	Description of Hybrid Defined Contribution Plan 166
Notes to Financial Statements	60	Description of Defined Contribution Plans Investment Options 167
Schedule of Employers' Net Pension Liability by System and Plan	77	Investment Option Performance Summary: Defined Contribution Plans 171
Schedule of Actuarial Methods and Significant Assumptions: Pension Plans	78	
Schedule of Impact of Changes in Discount Rate: Pension Plans	79	
Schedule of Participating Employers: OPEB Plans	81	

(Continued)

Audit Objectives

- **Virginia ACFR**
 - Objective of audit is also to ensure fair presentation of attachments and supplemental items submitted to DOA
 - Inquiries often require communication between VRS, DOA, and their respective audit teams
 - The VRS audit PM performs final review for both projects to ensure consistency
 - Team also considers internal control processes relating to the compilation of this information



Audit Objectives

- **Required Supplementary Information (RSI)**
 - We review for consistency with the basic financial statements
 - We perform limited procedures, including management inquiries and review of support
 - We do not provide an opinion concerning RSI

1. INTRODUCTORY SECTION		
Chair's Letter	9	Schedule of Employers' Net OPEB Liability by Program and Plan 87
Board of Trustees	14	Schedule of Actuarial Methods and Significant Assumptions: OPEB Plans 88
VRS Organization	15	Schedule of Impact of Changes in Discount Rate: LODA Plan 89
Investment Advisory Committee	15	Schedule of Impact of Changes in Health Care Trend Rate: LODA Plan 89
Defined Contribution Plans Advisory Committee	15	Schedule of Impact of Changes in Discount Rate: Non-LODA OPEB Plans 90
Executive Administrative Team	16	
Executive Investment Team	16	
Professional Consultants	16	
Letter of Transmittal	17	
2. FINANCIAL SECTION		
Independent Auditor's Report	31	Required Supplementary Schedule of Changes in Employers' Net Pension Liability: VRS State 116
Management's Discussion and Analysis	35	Required Supplementary Schedule of Changes in Employers' Net Pension Liability: VRS Teacher 118
Basic Financial Statements:	46	Required Supplementary Schedule of Changes in Employers' Net Pension Liability: VRS Political Subdivisions 120
VRS Statement of Fiduciary Net Position: Defined Benefit Pension Trust Funds and Other Employee Benefit Trust Funds	46	Required Supplementary Schedule of Changes in Employers' Net Pension Liability: SPORS 122
VRS Statement of Changes in Fiduciary Net Position: Defined Benefit Pension Trust Funds and Other Employee Benefit Trust Funds	47	Required Supplementary Schedule of Changes in Employers' Net Pension Liability: VaLORS 124
VRS Statement of Fiduciary Net Position: Defined Benefit Pension Trust Funds	48	Required Supplementary Schedule of Changes in Employers' Net Pension Liability: JRS 126
VRS Statement of Changes in Fiduciary Net Position: Defined Benefit Pension Trust Funds	49	Required Supplementary Schedule of Employer Contributions: Pension Plans 128
VRS Combining Statement of Fiduciary Net Position	50	Required Supplementary Schedule of Investment Returns 129
VRS Combining Statement of Changes in Fiduciary Net Position	51	Required Supplementary Schedule of Changes in Employers' Net OPEB Liability and Related Ratios 130
VRS Combining Statement of Fiduciary Net Position: Other Employee Benefit Trust Funds	52	Required Supplementary Schedule of Employer Contributions: OPEB Plans 141
VRS Combining Statement of Changes in Fiduciary Net Position: Other Employee Benefit Trust Funds	53	Schedule of Investment Expenses 144
Retiree Health Insurance Credit Combining Statement of Fiduciary Net Position	54	Schedule of Administrative Expenses 145
Retiree Health Insurance Credit Combining Statement of Changes in Fiduciary Net Position	55	Schedule of Professional and Consulting Services 146
VLDP Combining Statement of Fiduciary Net Position	56	
VLDP Combining Statement of Changes in Fiduciary Net Position	57	3. INVESTMENT SECTION
VRS Statement of Fiduciary Net Position: Other Custodial Plans	58	Chief Investment Officer's Letter 149
VRS Statement of Changes in Fiduciary Net Position: Other Custodial Plans	58	Investment Account 153
Notes to Financial Statements	60	Portfolio Highlights 155
Schedule of Employers' Net Pension Liability by System and Plan	77	VRS Money Managers 161
Schedule of Actuarial Methods and Significant Assumptions: Pension Plans	78	Public Equity Commissions 164
Schedule of Impact of Changes in Discount Rate: Pension Plans	79	Schedule of Investment Expenses 164
Schedule of Participating Employers: OPEB Plans	81	Investment Summary 165
		Description of Hybrid Defined Contribution Plan 166
		Description of Defined Contribution Plans Investment Options 167
		Investment Option Performance Summary: Defined Contribution Plans 171

(Continued)

Audit Objectives

- **Supplementary Information**
 - We provide an opinion that schedules are fairly stated ‘in relation to’ the basic financial statements
 - We reconcile the total schedule amount to the basic financial statements and sub-amounts to the general ledger system
 - We perform limited additional procedures, including management inquiries

1. INTRODUCTORY SECTION		Schedule of Employers’ Net OPEB Liability by Program and Plan	87
Chair’s Letter	9	Schedule of Actuarial Methods and Significant Assumptions: OPEB Plans	88
Board of Trustees	14	Schedule of Impact of Changes in Discount Rate: LODA Plan	89
VRS Organization	15	Schedule of Impact of Changes in Health Care Trend Rate: LODA Plan	89
Investment Advisory Committee	15	Schedule of Impact of Changes in Discount Rate: Non-LODA OPEB Plans	90
Defined Contribution Plans Advisory Committee	16	Required Supplementary Schedule of Changes in Employers’ Net Pension Liability: VRS State	116
Executive Administrative Team	16	Required Supplementary Schedule of Changes in Employers’ Net Pension Liability: VRS Teacher	118
Executive Investment Team	16	Required Supplementary Schedule of Changes in Employers’ Net Pension Liability: VRS Political Subdivisions	120
Professional Consultants	16	Required Supplementary Schedule of Changes in Employers’ Net Pension Liability: SPORS	122
Letter of Transmittal	17	Required Supplementary Schedule of Changes in Employers’ Net Pension Liability: VaLORS	124
2. FINANCIAL SECTION		Required Supplementary Schedule of Changes in Employers’ Net Pension Liability: JRS	126
Independent Auditor’s Report	31	Required Supplementary Schedule of Employer Contributions: Pension Plans	128
Management’s Discussion and Analysis	35	Required Supplementary Schedule of Investment Returns	129
Basic Financial Statements:	46	Required Supplementary Schedule of Changes in Employers’ Net OPEB Liability and Related Ratios	130
VRS Statement of Fiduciary Net Position: Defined Benefit Pension Trust Funds and Other Employee Benefit Trust Funds	46	Required Supplementary Schedule of Employer Contributions: OPEB Plans	141
VRS Statement of Changes in Fiduciary Net Position: Defined Benefit Pension Trust Funds and Other Employee Benefit Trust Funds	47	Schedule of Investment Expenses	144
VRS Statement of Fiduciary Net Position: Defined Benefit Pension Trust Funds	48	Schedule of Administrative Expenses	145
VRS Statement of Changes in Fiduciary Net Position: Defined Benefit Pension Trust Funds	49	Schedule of Professional and Consulting Services	146
VRS Combining Statement of Fiduciary Net Position	50	3. INVESTMENT SECTION	
VRS Combining Statement of Changes in Fiduciary Net Position	51	Chief Investment Officer’s Letter	149
VRS Combining Statement of Fiduciary Net Position: Other Employee Benefit Trust Funds	52	Investment Account	153
VRS Combining Statement of Changes in Fiduciary Net Position: Other Employee Benefit Trust Funds	53	Portfolio Highlights	155
Retiree Health Insurance Credit Combining Statement of Fiduciary Net Position	54	VRS Money Managers	161
Retiree Health Insurance Credit Combining Statement of Changes in Fiduciary Net Position	55	Public Equity Commissions	164
VLDP Combining Statement of Fiduciary Net Position	56	Schedule of Investment Expenses	164
VLDP Combining Statement of Changes in Fiduciary Net Position	57	Investment Summary	165
VRS Statement of Fiduciary Net Position: Other Custodial Plans	58	Description of Hybrid Defined Contribution Plan	166
VRS Statement of Changes in Fiduciary Net Position: Other Custodial Plans	58	Description of Defined Contribution Plans Investment Options	167
Notes to Financial Statements	60	Investment Option Performance Summary: Defined Contribution Plans	171
Schedule of Employers’ Net Pension Liability by System and Plan	77		
Schedule of Actuarial Methods and Significant Assumptions: Pension Plans	78		
Schedule of Impact of Changes in Discount Rate: Pension Plans	79		
Schedule of Participating Employers: OPEB Plans	81		

(Continued)

Audit Objectives

- **Other Information**
 - We review for inconsistency with the basic financial statements
 - We review for apparent material misstatements of fact based on knowledge of operations
 - We do not provide an opinion or any assurance whatsoever concerning other information

1. INTRODUCTORY SECTION		3. INVESTMENT SECTION	
Chair's Letter	9	Chief Investment Officer's Letter	149
Board of Trustees	14	Investment Account	153
VRS Organization	15	Portfolio Highlights	155
Investment Advisory Committee	15	VRS Money Managers	161
Defined Contribution Plans Advisory Committee	15	Public Equity Commissions	164
Executive Administrative Team	16	Schedule of Investment Expenses	164
Executive Investment Team	16	Investment Summary	165
Professional Consultants	16	Description of Hybrid Defined Contribution Plan	166
Letter of Transmittal	17	Description of Defined Contribution Plans Investment Options	167
		Investment Option Performance Summary: Defined Contribution Plans	171
4. ACTUARIAL SECTION		5. STATISTICAL SECTION	
Pension Trust Funds:		VRS Fiscal Year Returns	261
Actuary's Certification Letter: Pension Plans	175	Pension Trust Funds:	
Summary of Actuarial Assumptions and Methods: Pension Plans	178	Schedule of Retirement Contributions by System and Plan	266
Solvency Test: Pension Plans	179	Schedule of Pension Trust Fund Additions by Source	267
Solvency Test: VRS Pension Plans	180	Schedule of Pension Trust Fund Deductions by Type	268
Schedule of Funding (Actuarial Value Basis): All Pension Plans	181	Schedule of Retirement Benefits by System and Plan	269
Schedule of Funding (Actuarial Value Basis): VRS Pension Plans	182	Schedule of Retirement Benefits by Type	269
Schedule of Active Member Valuation Data: Pension Plans	183	Schedule of Refunds by Type	271
Schedule of Active Member Valuation Data: VRS Pension Plans	184	Schedule of Retirees and Beneficiaries by Type of Retirement and Plan	274
Schedule of Retiree and Beneficiary Valuation Data: Pension Plans	185	Schedule of Retirees and Beneficiaries by Type of Retirement and Plan	274
Schedule of Retiree and Beneficiary Valuation Data: VRS Pension Plans	186	Schedule of Retirees and Beneficiaries by Payout Option Selected	275
Actuarial Assumptions and Methods	189	Schedule of Average Benefit Payments	275
Additional Information About Actuarial Assumptions and Methods: Pension Plans	209	Schedule of Funding (Market Value Basis): All Pension Plans	284
Summary of Pension Plan Provisions	210	Schedule of Funding (Market Value Basis): VRS Pension Plans	285
Summary of Pension Plan Changes	219	Other Employee Benefit Trust Funds:	
Other Post-Employment Benefit (OPEB) Plan Funds:		Schedule of Group Life Insurance Additions by Source	287
Actuary's Certification Letter: OPEB Plans	221	Schedule of Group Life Insurance Deductions by Type	287
Actuary's Certification Letter: OPEB Plans – Line of Duty Act Fund	224	Schedule of Retiree Health Insurance Credit Additions by Source	291
Summary of Actuarial Assumptions and Methods: OPEB Plans	227	Schedule of Retiree Health Insurance Credit Deductions by Type	292
Solvency Test: OPEB Plans	228	Schedule of Disability Insurance Trust Fund Additions by Source	293
Schedule of Active Member Valuation Data: OPEB Plans	230	Schedule of Disability Insurance Trust Fund Deductions by Type	294
Schedule of Retiree and Beneficiary Valuation Data: OPEB Plans	232	Schedule of Retired Members and Beneficiaries by Plan	297
Additional Information About Actuarial Assumptions and Methods: OPEB Plans	252	Schedule of Average Benefit Payments by Plan	297
Summary of OPEB Plan Provisions	254	VRS-Participating Employers	299
Summary of OPEB Plan Changes	258	Hybrid Defined Contribution Plan Schedules	306
		Commonwealth of Virginia 457 Deferred Compensation and Cash Match Plans	307

Approach to Materiality

- We consider what is likely to affect the judgment of a financial statement user in order to:
 - Assess risk and design audit procedures
 - Evaluate misstatements in amounts and deficiencies in processes
- Includes quantitative and qualitative considerations
- Certain procedures are performed at a lower level of materiality in preparation for the employer-level opinions provided in support of Employer Assurances Engagement

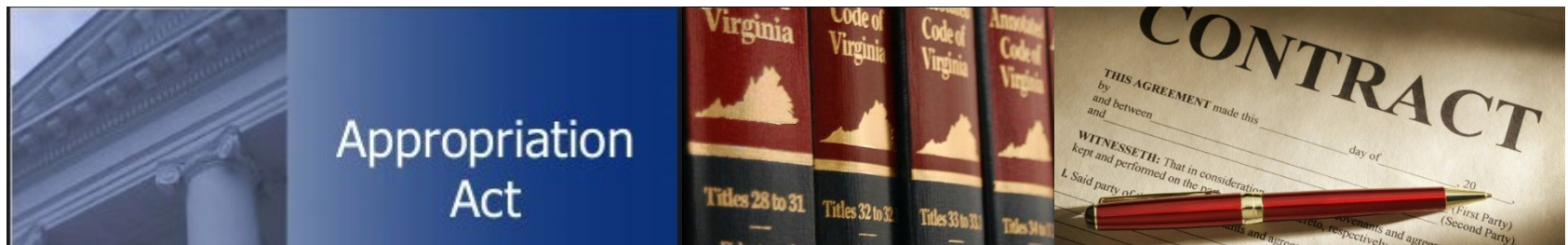
Approach to Fraud

- Team interviews personnel and assesses the risk of fraud
- Team looks for red flags and considers the potential for fraud as it relates to exceptions identified during fieldwork
- VRS is required to notify APA when fraud is identified



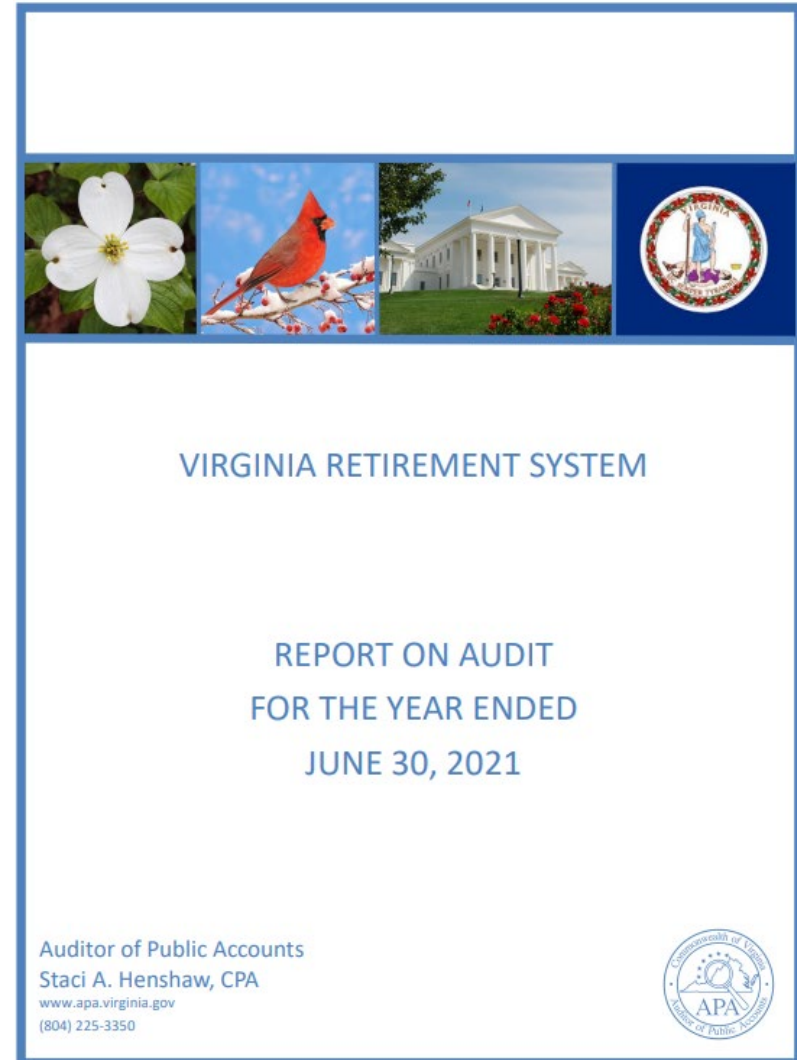
Approach to Compliance

- We consider the risk that potential non-compliance could have a material direct or indirect effect on the financial statements
- We assess management's processes
- We test compliance which we deem significant in the context of the audit objectives



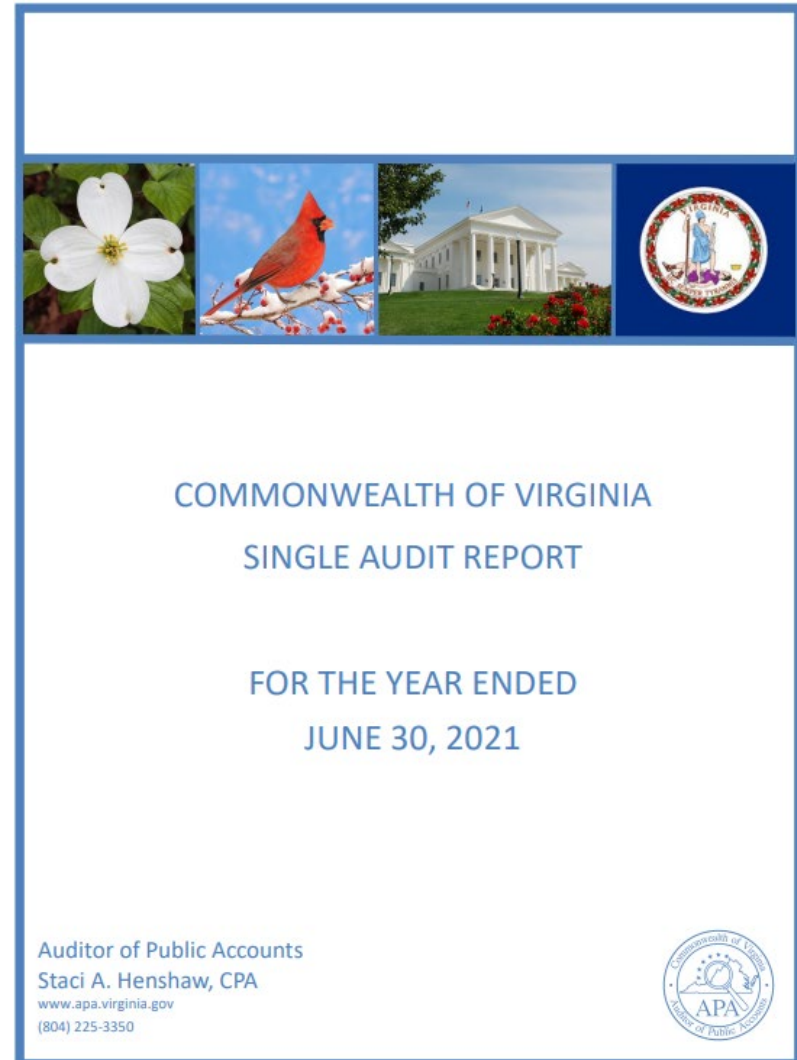
Audit Objectives

- **Report on Internal Controls and Compliance**
 - We do not provide an opinion on internal controls
 - We are required to report any findings that we deem to be significant deficiencies or material weaknesses
 - Though not required, we plan to issue this report the same week we release the audit opinion



Audit Objectives

- **Statewide Single Audit**
 - The Statewide Single Audit (SSA) report serves as the internal control report for the Commonwealth's Annual Comprehensive Financial Report
 - Findings included in the VRS internal controls report will be carried forward to the SSA report
 - VRS did not have any prior year findings requiring follow up



Management Communication

- Entrance/Exit with Management
- Bi-weekly status meetings:
 - Financial
 - Investments
- When potential concerns are noted:
 - Confirm condition
 - Obtain response
 - Evaluate significance

Audit Committee Communication

- If you are aware of risks our audit should address, please share those with us
- Unless there are findings requiring your immediate attention, we will present our results to you at the conclusion of the audit
- If earlier communication is warranted, we will coordinate with internal audit to ensure the Committee is informed in a timely manner
- Terms of the engagement and representation letters will be provided

Intended Use Statement

This presentation is intended solely for the information and use of those charged with governance and management, and is not intended to be, and should not be, used by anyone other than these specified parties.

Audit Reports

Cash Management

For the period October 1, 2021, through January 1, 2022

Highlighting VRS Core Values: *Integrity, Teamwork, Accountability* and *Agility* in Action

THIS REPORT IS INTENDED SOLELY FOR THE USE OF THE VRS BOARD OF TRUSTEES AND THE MANAGEMENT OF VRS AND IS NOT INTENDED FOR OTHER PURPOSES.



TRANSMITTAL LETTER

May 12, 2022

Dear Members of the Audit and Compliance Committee,

We have completed audit number 443, "Cash Management." The main purpose of our audit was to review VRS' processes for cash management to determine if they support operational needs and comply with applicable statutory requirements.

We conducted our audit in accordance with the *International Standards for the Professional Practice of Internal Auditing*. These standards require that we plan and perform the audit to obtain sufficient and appropriate evidence to provide a reasonable basis for the conclusions based upon our audit objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

This report was distributed to the VRS Director, Chief Investment Officer and members of management for review and comment. As our review did not result in a written recommendation, management did not provide a written response but expressed substantial agreement with our report.

We appreciate the cooperation and assistance of the Finance and Investment Departments throughout this audit.

Respectfully Submitted,

A handwritten signature in black ink that reads 'Jennifer P. Bell Schreck'.

Jennifer P. Bell Schreck, CPA, CISA, PMP
Audit Director

TABLE OF CONTENTS

TITLE PAGE	1
TRANSMITTAL LETTER	2
EXECUTIVE SUMMARY	3
BACKGROUND	4
SCOPE AND METHODOLOGY	22
CONCLUSIONS	25
FOLLOW-UP ON PRIOR REPORTS	27
RECOMMENDATIONS	27
MANAGEMENT EXIT CONFERENCE	27
REPORT DISTRIBUTION	28
PRINCIPAL AUDITOR IN-CHARGE	28

EXECUTIVE SUMMARY

We conducted an examination of the Cash Management processes of the Virginia Retirement System (VRS) for the period October 1, 2021, through January 1, 2022. Our review determined that:

- Processes support operational needs and comply with applicable statutory requirements;
- Bank and investment accounts significant to cash management are adequately monitored; and
- Cash deposits are reasonably protected in the event of bank failure.

Our audit did not address cash deposits related to VRS' investment responsibility for custodial funds for the Volunteer Firefighters' and Rescue Squad Workers' Service Award Program (VolSAP) and separate bank accounts set up to support third party activities performed on VRS' behalf for the Virginia Sickness and Disability and Virginia Local Disability Programs.

There are no written recommendations resulting from our review.

SNAPSHOT

The VRS Finance and Investment Departments collaborate to monitor cash deposits and meet operational cash needs.

As of January 1, 2022, VRS cash deposits were \$1.05 Billion, approximately 1% of the Total Fund market value.

AUDIT ASSESSMENT

Cash management processes exist to support operational needs and comply with applicable statutory requirements.

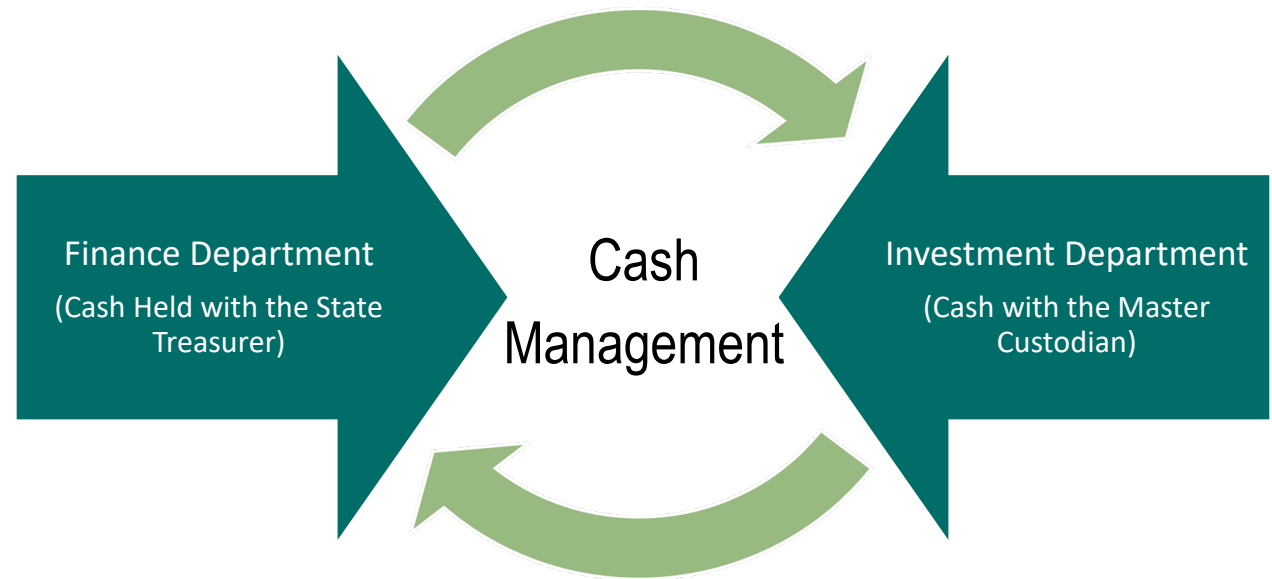
Written Recommendations: 0

BACKGROUND

INTRODUCTION

As of January 1, 2022, the Virginia Retirement System (VRS) had \$1.05 Billion in cash deposits. Primary sources of these deposits are the contributions received from members and employers and inflows related to investment management. Significant uses of cash include payment of retirement and other post-employment benefits, administrative expenses and investment management expenses.

VRS' Finance and Investment Departments collaborate in monitoring cash deposits to maintain balances sufficient to meet investment and administrative operational needs.



The Finance Department has the primary responsibility for monitoring cash deposits held with the State Treasurer, while the Investment Department monitors cash deposits held with VRS' master custodian, Bank of New York Mellon (BNYM). *Teamwork*, timely communication and coordination between both departments support holistic cash management across the organization by estimating and then transferring cash, as needed, in anticipation of operational and investment needs.

Cash Management Pg. 4 of 28

TOPICS OF INTEREST

As we consider VRS' **Cash Assets** and their **Management** to **support** VRS' **operating cash needs**, we will **discuss** the **following topics**:

- [Cash Deposits](#)
- [Protection of Cash Deposits](#)
- [Investment of Cash Deposits](#)
- [Cash Management](#)
- [Cash Related Reconciliations](#)
- [Cash Forecasting](#)

Activities and business processes to manage and monitor cash deposits support VRS' achievement of its mission "To deliver retirement and other benefits to Virginia public employees through sound financial stewardship and superior customer service." These activities and business processes are supported by policies, procedures and practices promoting *accountability* throughout the organization.

CASH DEPOSITS

VRS' cash deposits primarily are held with the State Treasurer and BNYM, the master custodian. Below are the cash deposits held with the State Treasurer and master custodian as of January 1, 2022, and as of June 30th for the three preceding fiscal years.

(EXPRESSED IN THOUSANDS)

	1/1/2022	6/30/2021	6/30/2020	6/30/2019
Cash held with the State Treasurer	\$ 530,339	\$ 48,494	\$58,746	\$ 45,732
Cash held with Master Custodian	521,120	97,212	8,581	74,743
Total	\$1,051,459	\$ 145,706	\$67,327	\$120,475

Sources: VRS Annual Reports for the Fiscal Years ending June 30, 2019-2021 and VRS general ledger as of 1/1/2022

These balances fluctuate frequently in response to the receipt, disbursement and transfer activities as part of VRS' daily operations, investment and cash management practices.

Virginia State Treasurer and Department of Treasury

VRS deposits held with the State Treasurer are comprised of trust and general cash. In accordance with the *Code of Virginia* [§ 2.2-1802](#) and [§ 2.2-1803](#), VRS' cash receipts, as public funds, are deposited to the credit of the State Treasurer in bank accounts held at a state authorized depository. VRS is responsible for complying with the State Treasurer's regulations or other directives for these deposits.

Organizational Authorization to Manage Cash

The VRS Board of Trustees' (Board) Resolution for Payment of Retirement System Funds in the State Treasury and Signing Official Documents designates persons employed at VRS and the State Treasurer who are authorized to sign vouchers for payments using VRS funds held with the State Treasurer.

This Board **resolution** also **designates** VRS **employees** who are **authorized** to **sign** VRS official documents, such as, but not limited to: **leases, deeds, contracts**, equity index **futures** and **options** on such futures, **signature cards**, **minutes** and **purchase orders**.

Generally, updates to such Board resolutions are related to a change in the Board Chair or turnover of VRS employees designated as authorized signers. This resolution was most recently updated on June 10, 2021.

Trust Cash

VRS has multiple bank accounts that can hold cash deposits, collectively referred to as “Trust Cash held with the State Treasurer”. Deposits in these accounts are referred to as “trust cash”, as cash in any of these accounts is part of the VRS Trust Fund.

The State Treasurer is authorized to view the account balances and activity, make payments from these accounts in accordance with the Board resolution previously discussed and move funds as needed to support VRS’ cash and short-term investment goals.

Over time, VRS has coordinated with Treasury to open additional bank accounts to enhance its cash management practices.

Each bank account has a distinct purpose and features to support the receipt, disbursement and transfer of VRS’ cash.

General Cash

In addition to trust cash, VRS also has General Cash held with the State Treasurer. This General Cash is reserved to make payments for VRS’ ongoing administrative and personnel expenses such as: employee payroll, office space and equipment expenses, etc. VRS’ General Cash is not held in a VRS designated bank account, rather it is held in one of the Commonwealth’s bank accounts collectively known as the Commonwealth’s General Account. The State Treasurer is responsible for accounting for VRS’ share of General Cash in its records, as the Commonwealth’s General Account contains General Cash held for other state agencies in addition to VRS.

VRS Code of Virginia Requirements

Code of Virginia [§ 51.1-150](#) states that cash, not to exceed ten percent of the total amount in the accounts of the retirement system, may be kept on deposit with the State Treasurer. VRS adheres to these statutory requirements through limits set on cash holdings by its internal policies as discussed later in the report.

Code of Virginia [§ 51.1-124.33](#) includes additional requirements for the Trust Fund for cash deposits not held for investment. Currently, all such VRS cash deposits for the Trust Fund are held

ASSET ALLOCATION FOR CASH

In **April 2020**, the **Board** **acknowledged** VRS' ongoing **need for cash** to meet operational needs by **formalizing** a **one percent asset allocation** for cash in the VRS Defined Benefit Plan **Investment Policy Statement**.

This change **reflects** the **presence** of cash in the Total Fund as a part of **normal operations**, while also **acknowledging** that it **should represent** a **limited** percentage **relative** to the **Total Fund** market value.

with the State Treasurer, with the State Treasurer ensuring conformance with these statutory requirements on VRS' behalf.

Cash Held with the Master Custodian

Any of VRS investment accounts with the master custodian may include cash balances, all of which is trust cash. Stated another way, as of a point in time, cash held with the master custodian consists of balances from various investment accounts across the entire Total Fund investment portfolio.

Organizational Authorization to Manage the Cash

Like the previous resolution, the VRS Board Resolution for Master Custodial Services designates VRS employees who are authorized to sign vouchers for asset transfers and account payments for VRS funds held with the master custodian. In addition, the resolution designates VRS employees who are authorized to open and close accounts, take administrative actions, sign proxies and sign for all actions involving compliance issues such as, but not limited to: class action suits, tax exemptions, authorized signatures, stock and bond powers and required resolutions as needed.

This resolution was last updated on June 10, 2021.

Limitations on Cash Holdings – VRS Policy

The governing document for the Total Fund is the VRS Defined Benefit Plan Investment Policy Statement. The current policy statement was updated and approved by the Board on November 14, 2018. Appendix 1 of the policy statement, which specifies the Total Fund asset classes and their respective policy targets, allowable ranges, benchmarks and tracking error ranges, was last updated and approved by the Board on July 1, 2021.

The appendix includes requirements for the cash asset class, as reflected in the table on the following page, applicable when evaluating the total cash that can be held in all investment accounts comprising the Total Fund investment portfolio and trust cash invested by Treasury in the Local Government Investment Pool (LGIP).

If cash has been earmarked for a specific purpose, such as derivatives and long and short investment activities, it is generally not classified as deposits given that the cash is not available to use for other purposes.

Asset Class	Policy Target %	Allowable Range	Benchmark
Cash	1.0%	0%-5%	Merrill Lynch 91-day T-Bill Index

The policy target percentage and allowable range reflected above support VRS' compliance with *Code of Virginia § 51.1-150* which provides that cash, not to exceed ten percent of the total amount in the accounts of the retirement system, may be kept on deposit with the State Treasurer.

While the VRS Defined Benefit Plan Investment Policy Statement establishes the parameters for total cash that can be held in the Total Fund, program and account-specific Investment Policy Statements provide further guidance regarding how much cash can be held and/or how cash can be invested as part of VRS' individual investment programs and strategies.

Compliance with the cash asset class requirements for the Total Fund is monitored through the Investment Department's review of the Daily Asset Allocation reports and through its cash forecasting activities. Additionally, cash deposits are considered as a function of the ongoing monitoring by the Investment Department for each investment program's allocation relative to the Total Fund. Compliance with program and account-specific requirements is managed at either the individual investment program or account level.

Independent of cash within individual investment accounts, VRS uses three specific investment accounts for cash management across the Total Fund as reflected in the table below.

Account	Investment Objective
BNYM VRS Cash Account	To maintain an adequate cash balance to meet the cash needs of the Investment Department.
BNYM VRS Rebalance Account	To maintain a reserve cash balance to meet the cash needs of the Investment Department and provide a short-term asset reallocation using equity and fixed income derivative securities.
Short-Term Investment Fund (STIF) Account	To provide a high level of current income consistent with low volatility of principal.

FEDERAL DEPOSIT INSURANCE CORPORATION

The **FDIC insures** deposits; **examines** and **supervises** financial institutions for **safety, soundness,** and **consumer protection**; makes large and complex financial institutions **resolvable**; and **manages receiverships** within the United States of America banking system.

PROTECTION OF CASH DEPOSITS

In the event of bank failure, recovery of cash deposits may be at risk. The Federal Deposit Insurance Corporation (FDIC) provides certain levels of assurance for their recovery and the *Code of Virginia* defines further requirements for insuring and collateralizing cash deposits for public funds as described below.

Federal Deposit Insurance Corporation

The FDIC is an independent agency created by the United States Congress to maintain stability and public confidence in the nation's financial system.

FDIC insurance is available for all bank accounts comprising Cash Held with the State Treasurer, with any deposits held in excess of FDIC coverage limits subject to the Security for Public Deposit Act discussed in the next section. In addition, FDIC insurance is also available for both cash held on deposit and cash swept into the STIF, held in qualifying accounts at the Master Custodian.

Under FDIC regulations, coverage is available on a pass-through basis to individual plan participants, up to a maximum limit of \$250,000 per participant, with the actual coverage at any point in time dependent on the number of affected plan participants and the underlying value of their accrued benefits.

In the event of bank failure, the claims process is automatic and does not require any submissions from VRS or other claimants in order to trigger a claim. The FDIC will affirmatively reach out to the Virginia Department of Treasury and/or VRS with any questions.

Once cash is no longer held in a qualifying deposit account, FDIC insurance coverage ceases. Generally, this occurs when the cash is invested or swept into a non-qualifying account. In a liquidation scenario, there are certain other situations that may impact FDIC coverage.

Security for Public Deposits Act

In addition, for Cash Held with the State Treasurer, deposits held in excess of the FDIC insurance coverage are collateralized in accordance with the Security for Public Deposits Act (SPDA) defined through [§§ 2.2-4400 through 2.2-4411](#) of the *Code of Virginia*. To collateralize these accounts, financial institutions designated as a qualified public depository pledge securities to be held by a custodian for the benefit of Virginia public depositors.

The Virginia Department of Treasury administers the SPDA, which involves ensuring qualified public depositories comply with the reporting and collateral requirements on behalf of all public depositors. For a financial institution to be classified as a qualified public depository, it must be authorized by the Treasury Board to hold Virginia public deposits in accordance with the SPDA. In the event of bank failure, the Virginia Department of Treasury is responsible for recovering funds for the SPDA and on the behalf of Virginia public depositors, including VRS.

VRS cash may be classified as a public deposit or an investment. All cash classified as a public deposit must be deposited in a qualified public depository. VRS deposits such cash through Virginia Department of Treasury accounts to fulfill this *Code of Virginia* requirement.

Once Cash Held with the Treasurer is no longer on deposit at a qualified public depository, coverage provided by the SPDA ceases. Generally, coverage ceases when Cash Held with the State Treasurer is invested or is no longer on deposit at a qualified public depository.

INVESTMENT OF CASH DEPOSITS

VRS continuously works to minimize its cash deposits in order to maximize its investment returns for the Trust Fund. As a result, short-term investment vehicles are used to earn income on cash balances until the funds are needed to meet current obligations. Maintaining *agility* in the short-term investment of cash allows VRS to earn income while keeping the funds readily available to meet operational and investment needs.

Investment of Cash Deposits - State Treasurer

In accordance with the *Code of Virginia* [§ 2.2-1806](#), the Governor and State Treasurer may, whenever there are funds in the State Treasury in excess of the amount required to meet the current needs and demands of the Commonwealth, invest the excess funds in securities that are legal investments under the laws of the Commonwealth for public funds. The funds shall be invested in such said securities as, in their judgment, will be readily convertible into cash. As such, when VRS does not need cash to meet its current needs and demands, the State Treasurer has the authority to invest it.

COMMONWEALTH GENERAL ACCOUNT

The **General Account portfolio** is the **largest managed** by the State Treasurer. The **largest funds** in the General Account are the **General Fund**, the **Transportation Trust Fund**, the **Highway Maintenance Fund**, the **Lottery Fund** and **various Insurance Funds**.

By **pooling** assets, the State Treasurer is able to **structure** a more **ambitious** and **dynamic investment program** for all fund participants.

The State Treasurer invests VRS cash into different portfolios aligned with the cash’s intended use: VRS’ Trust Cash is invested into the LGIP and VRS’ General Cash is invested into the General Account.

General Account

As discussed previously, the *Code of Virginia* authorizes the State Treasurer to invest the operating funds, i.e., General Cash, in the Commonwealth’s General Account portfolio on the behalf of all state agencies, including VRS, until they are needed to meet current obligations. The State Treasurer manages these investments in the Commonwealth’s General Account portfolio. Investment earnings for cash invested by the State Treasurer in the General Account portfolio is not allocated back to state agencies, it is retained by the Commonwealth. As such, VRS works to minimize its General Cash held with the State Treasurer.

From VRS’ perspective, the Commonwealth General Account is simply another bank account holding cash that is available and designated for use in paying VRS agency operating expenses.

Local Government Investment Pool

In accordance with the Local Government Investment Pool Act (*Code of Virginia §§ 2.2-4600 through 2.2-4606*), the Treasury Board administers the LGIP which aggregates and invests public funds placed in the custody of the State Treasurer. As a voluntary participant in the LGIP, VRS has its own account. The State Treasurer invests trust cash on VRS’ behalf when VRS does not require the cash to meet current needs such as paying retirement and other post-employment benefits. VRS receives the investment income based on the holdings of its LGIP account within the investment pool.

(EXPRESSED IN THOUSANDS)

	1/1/2022
LGIP Account Market Value	\$ 46,441

Source: LGIP account statement and VRS general ledger

Investment of Cash Deposits – Master Custodian

As previously noted, the VRS Defined Benefit Plan Investment Policy Statement coupled with Program Investment Policy Statements and/or account level Investment Advisory Agreements authorize how cash deposits held at BNYM may be invested. For example, the Investment Policy

Statements for the BNYM VRS Cash account and BNYM VRS Rebalance account and the Investment Advisory Agreement for the STIF account specify allowable securities and transactions. The table below as of January 1, 2022, represents the non-cash holdings of these accounts.

(EXPRESSED IN THOUSANDS)

	1/1/2022
STIF Account	\$4,746,228
BNYM VRS Cash Account	\$1,186,146
BNYM Rebalance Account	\$111,750

Source: BNYM Records: Net Assets, excluding cash deposits

CASH MANAGEMENT

Responsibility for the daily management of accounts with significant cash balances or activity is shared among VRS, the State Treasurer and the investment manager for the STIF account. Cash transfers occur frequently for the deposits held with the State Treasurer and BNYM. Transfers enable cash to be moved from one account to another to support ongoing operational and investment needs.

Cash Held with the State Treasurer

Transfers among Trust Cash Bank Accounts & LGIP

As part of managing the VRS Trust cash and in accordance with each bank account’s purpose and features, the State Treasurer will transfer cash, moving it among accounts to support either making benefit plan related payments or investing cash deposits into the LGIP.

VRS Administrative and Personnel Expenses

Monthly, VRS transfers 1/12 of its appropriated operating budget from Trust Cash held with the State Treasurer to the Commonwealth’s General Account. This transfer ensures sufficient cash exists in the Commonwealth’s General Account to pay VRS administrative and personnel expenses. At its discretion, the State Treasurer may then transfer cash from the Commonwealth’s General Account into the Commonwealth’s General Account Portfolio for investment.

Managing Individual Fund Shares of General Cash – VRS Monthly Cash Sweep Vouchers

VRS General Accounting prepares monthly cash sweep vouchers to bring General Cash balances at the individual fund level to a zero. This applies to all accounting funds recorded in VRS' general ledger except for the VRS Administrative Fund.

Typically, the net effect of each fund's combined monthly wires results in a net transfer of cash from the Commonwealth's General account to Trust Cash held with the State Treasurer. This allows VRS' trust cash to be invested to the benefit of the Trust Fund through the LGIP until VRS needs the funds to make benefit payments.

It is possible for the net effect of these monthly wires to result in a positive amount of cash being transferred from Trust Cash held with the State Treasurer to the Commonwealth's General Account. However, historically this has not been common, as VRS' net cash flows recorded for the Commonwealth's General Account typically outpace net cash flows recorded to Trust Cash held with the State Treasurer.

Cash Held with the Master Custodian

Accounts

BNYM VRS Cash Account

The VRS BNYM Cash account is managed internally by the VRS Investment Department and serves as the primary cash account for investments. Excess cash in this account is permitted to be marketized by using equity and fixed income securities.

BNYM VRS Rebalance Account

Designated members of the VRS Internal Equity Management, Fixed Income and Portfolio Solutions Group Teams are authorized to serve as the Rebalance Account Team and collaborate to make investment decisions and execute day-to-day management of the VRS BNYM Rebalance account. As part of its account management responsibilities, the Fixed Income Team manages any fixed income exposures in the account.

STIF Account

VRS has engaged an investment manager for the STIF account. This account serves as an investment vehicle for cash deposits in all investment accounts comprising the Total Fund. Each business day, cash is swept into the account to purchase shares in the STIF held overnight and

Cash Management Pg. 13 of 28

VRS STIF ACCOUNT HISTORY

Prior to 2015, VRS used existing **prime money market** and **federal funds money** market accounts, moving between the two **based** on **risk tolerance** as a means for **short-term investment** of cash.

In 2015, the **VRS Fixed Income team** proposed **establishing** a **STIF account** to serve as short-term investment vehicle for cash.

This **change provided** VRS with the **opportunity** to **negotiate** the **terms of account management**, including **lower fees** and **higher yields**.

Since its **inception** in January 2015 through January 2022, the VRS STIF account has had an average:

lower expense ratio of
0.14%

higher net yield of
0.32%

outright yield difference of
0.18%

then swept back into the investment accounts from which the cash originated so it is available for use during market hours.

VRS has an Investment Advisory Agreement (last updated March 2015) with the investment manager which specifies duration and asset guidelines, asset allocations, credit criteria, benchmark and other investment practices. For performance reporting, earnings from the STIF account are applied back to the underlying investment accounts from which the invested cash originated.

As a Total Fund account, the Investment Department has assigned oversight for the STIF to the VRS Fixed Income Team.

Cash Transfers

Cash transfers are used throughout the Investment Department to support managing the Total Fund in accordance with the VRS Defined Benefit Plan Investment Policy Statement and each Program's or account's Investment Policy Statement and/or Investment Advisory Agreement. Cash management for these accounts is further supported by VRS' Investment Accounting, Compliance and Operations Departments.

Additionally, monthly the Investment Department will transfer funds from the BNYM VRS Cash account or BNYM VRS Rebalance account to Cash Held with the State Treasurer to ensure sufficient funds exist to meet the Trust's financial obligations to its members, retirees and beneficiaries. In recent years, the transfer has been funded predominantly from the BNYM VRS Cash account, as cash deposits in the BNYM VRS Rebalance account have been reserved to use for investment purposes.

Direction Letters to Initiate Transfers

A direction letter is prepared by Investment Accounting for all cash transfers (i.e., capital calls, outgoing payments, movement of cash among VRS accounts, etc.) requested by the Investment Department staff. Investment Accounting obtains approval from the requestor(s) and from an authorized signer from the Investment Department before emailing the direction letter to the Control Team within the Finance Department who handles obtaining approval of the authorized signer from Administration and sends the direction letters to BNYM for processing after all signatures are obtained.

SOFT DOLLARS AND BEST EXECUTION

Soft dollars are a means of **paying brokerage** firms for their **services** through **commission revenue**, as opposed to through normal **direct payments**.

VRS defines **best execution** as the **process and price** that **results** in the **best overall performance impact**, considering **current** market **conditions**.

Compliance with the Investment Policy Statements

Portfolio Management Software

VRS contracts for use of a portfolio management software which, as part of its features, includes compliance monitoring with Investment Policy Statement requirements and exchanging data with various pricing sources. VRS also uses this software to support automated reconciliations of cash and positions with BNYM.

BNYM VRS Cash and Rebalance Accounts

Internally, for the BNYM VRS Cash and Rebalance accounts, the Investment Department monitors compliance with each account's Investment Policy Statement and Internal Equity Management's Investment Policy Statement by using rules programmed into the portfolio management software. The rules are applied pre-trade as a Portfolio Manager enters an order and then again after the order is executed. Investment Compliance personnel monitor exceptions to rules in the portfolio management software and work with the applicable Portfolio Managers and the Trading Desk to research and resolve.

Additionally, designated members of the Investment Department perform portfolio risk analyses and monitor trading activity for best execution. VRS Investment Department personnel do not engage in third party soft dollar arrangements for these accounts.

STIF Account

The investment manager has access to the STIF account information in the portfolio management software and is responsible for maintaining any compliance rules and monitoring for exceptions; however, in the software the VRS Investment Department is able to view daily activity and balances for the STIF account.

The VRS Investment Department relies on viewing daily activity in the portfolio management software and the Fixed Income Team performing a monthly portfolio risk analysis and review of investment manager's compliance with guidelines and criteria included in the Investment Advisory Agreement. Additional due diligence activities include but are not limited to the Fixed Income Team meeting annually with the investment manager to discuss the portfolio, cash market and other relevant information for the account.

The investment manager is responsible for monitoring its trade activity for best execution in accordance with the terms of the Investment Advisory Agreement. The investment manager is permitted to generate soft dollars to be used by them on behalf of VRS but is required to disclose all material soft dollar expenditures at fiscal year end in excess of \$10,000 to VRS in accordance with *Code of Virginia § 51.1-1000.3.A*.

Monthly Performance Reporting

BNYM generates monthly performance reports for all asset classes which are reviewed and approved by the respective program directors or designees. The monthly performance report for the VRS Rebalance account is reviewed and approved by the Managing Director of the Portfolio Solutions Group. Monthly performance for the VRS Cash and STIF accounts is reported as part of the Total Fund, which is reviewed and approved by the Chief Administrative Officer and Chief Investment Officer.

CASH RELATED RECONCILIATIONS

The VRS Finance and Investment Departments perform various reconciliation processes to support the accuracy, completeness and *integrity* of recorded cash transactions and balances.

Cash Held with the Treasurer

Bank Account Reconciliations – Trust Cash

The VRS Finance Department and Department of Treasury staff perform separate reconciliations to support the accuracy and completeness of the balances and activity for the bank accounts comprising Trust Cash held with the State Treasurer. The VRS Finance Department and Treasury personnel communicate regularly to identify and resolve reconciling differences between their records throughout the month.

The VRS Finance Department performs reconciliations as of month-end for each bank account, comparing activity and balances recorded in VRS' general ledger to the reports provided by Treasury. Bank and LGIP statements may be used as resources in researching and reconciling differences. Treasury performs daily reconciliations by comparing activity and balances recorded in its general ledger to the Commonwealth's general ledger, with which VRS' general ledger interfaces daily, allowing Treasury personnel to view VRS' accounting entries.

Due to and Due from Reconciliations

The VRS Finance Department performs a monthly reconciliation the day of Commonwealth's general ledger monthly pre-close to prepare the VRS general ledger for final close. This reconciliation ensures journal entries have been recorded properly related to amounts "due to" and "due from" for all VRS funds. It occurs prior to the monthly distribution of investment income from the Total Fund portfolio and supports the accurate completion of the monthly cash sweep vouchers.

Cash Held with the Master Custodian

BNYM serves an integral role as VRS' master custodian by maintaining the official accounting records for all investments and providing security settlement processing, asset custody and income collection, as well as other investment and accounting related services. VRS, the STIF investment manager and BNYM perform various reconciliation processes to support the accuracy and completeness of recorded cash transactions and balances.

Daily

For the BNYM VRS Rebalance account, the portfolio management software performs automated reconciliations of its records for cash and positions to BNYM records. The software will generate exceptions for identified differences. For the BNYM VRS Cash account, a daily reconciliation is performed in the Cash Database.

Trading and other activities done in the portfolio management software are not dependent on the resolution of exceptions generated from these reconciliations.

VRS Investment Operations researches and resolves exceptions for BNYM VRS Cash account, while the portfolio management software vendor researches and resolves exceptions for the BNYM VRS Rebalance account and the investment manager does the same for the STIF account per their contracts with VRS.

Monthly - BNYM

BNYM performs a review of all investment accounts by comparing investment positions and valuations recorded in BNYM's records with those reported by the investment manager or VRS staff. Discrepancies related to missing or stale prices or prices which fail pre-established account

tolerance checks are researched and resolved with the investment manager or Investment Operations. Other discrepancies reviewed may include those related to differences in accounting or accrual methods.

Monthly – Investment Operations – BNYM VRS Cash Account

Investment Operations reconciles cash and holdings for the BNYM VRS Cash account by comparing the information recorded in VRS' internal records to BNYM records. VRS' internal records of activity in the VRS Cash account are maintained in the Cash Database updated each day by Investment Operations staff, using direction letters and other documentation supporting activity occurring in the BNYM VRS Cash account.

Monthly – Investment Operations – BNYM VRS Rebalance Account

VRS contracts with the portfolio management software vendor to perform monthly net asset valuation reconciliations between the portfolio management software and BNYM records for the BNYM VRS Rebalance account. Upon receiving the reconciliation performed by the portfolio management software vendor, Investment Operations performs a high-level review and comparison of the information to BNYM records for reasonableness.

Monthly – Investment Accounting

Each month Investment Accounting reconciles all balances recorded in BNYM's records on a consolidated basis to the VRS general ledger.

Quarterly – Investment Accounting – BNYM VRS Cash, BNYM VRS Rebalance, and STIF Accounts

Investment Accounting receives the reconciliations prepared by each investment manager, Investment Operations, or the portfolio management software vendor as of quarter end for all VRS investment accounts. Investment Accounting reviews the reconciliations to ensure the balances identified as being from BNYM are consistent with BNYM reports and checks for any unusual items listed on the reconciliations, following up as needed with the responsible party. Investment Accounting completes a quarterly reconciliation checklist documenting its review of all reconciliations received and distributes it to members of the Investment Department, the Chief Financial Officer and Program Directors.

All Cash Deposits (VRS General Ledger to Commonwealth General Ledger) - Monthly

The VRS Finance Department performs a monthly reconciliation to ensure all entries for the individual funds in VRS' general ledger system have posted to the Commonwealth's general ledger system. Balances and activity for all cash deposits, both held by the master custodian and State Treasurer, are reconciled as part of this process. Any entries not shown in both the VRS general ledger and the Commonwealth's general ledger system are researched as reconciling items.

CASH FORECASTING

Cash forecasting activities performed by the VRS Investment and Finance Departments start with collecting and aggregating data that serve as inputs into projecting cash needs and cash deposits available for use. This information allows VRS to proactively identify accounts with cash shortfalls that will require a transfer from another account to meet cash needs.

Forecasting Organizational Cash Needs

The Investment Department has developed an in-house database and modeling tools to assist with monitoring current cash balances and future cash activity.

Each business day, the Investment Department monitors cash deposits held with the master custodian, predominantly in the BNYM VRS Cash account and BNYM VRS Rebalance account. Monitoring activities support forecasting how cash will fluctuate in relation to the management of the Total Fund portfolio and agency operational cash needs. The Investment Department draws cash mainly from the BNYM VRS Cash account for operational cash needs, as the other cash balances are reserved for specific investment purposes.

Cash Database

VRS utilizes the Cash Database specifically to track daily activity and balances for the BNYM VRS Cash account. The Cash Database is considered to be the source of VRS' internal records for the account. Transaction details are typically obtained from notices for capital calls and distributions, direction letters and other information related to the account that Investment Operations receives via email from other Investment Department personnel. The transactions may relate to current or future cash activity. Validation controls are built into the database, and transactions are reconciled daily to BNYM reports.

MODEL SCOPE

The **Model** looks **beyond** the **BNYM VRS Cash account** to include **other significant cash activity** and **holdings**, including the BNYM VRS **Rebalance account**, cash held as **collateral**, **Trust Cash** held **with** the **State Treasurer** and cash **holdings for transition accounts**.

Each business day, Cash Database activity reports are distributed to the investment manager for the STIF account, Investment Operations and other Investment Department personnel as appropriate. These reports assist with the validation of the Cash Database, management of the STIF account and overall management of cash within the Total Fund portfolio.

VRS Rebal Global Model

The Investment Department uses the VRS Rebal Global Model (the Model) to holistically monitor cash by providing a forward-looking view of cash flows, physical cash holdings and cash exposures for the Total Fund portfolio.

The Cash Database, along with data provided by other vendor applications and BNYM market value data feeds the Model. These persistent connections allow updates to be captured in real-time and minimize manual data entry. Investment Department personnel periodically compare data in the Model independently to data sources as a data quality check. This facilitates the daily analysis of the data in relation to current asset class total market values, impacts of overlays and weights required by the VRS Defined Benefit Plan Investment Policy Statement.

When the Model identifies a need to raise cash for the Total Fund portfolio, be it for investment or operational purposes, relevant data and observations are submitted to the Investment Department Executive Committee for review. Impacts of the cash raise on Total Fund asset classes are considered relative to the target asset allocations and allowable ranges in the VRS Defined Benefit Plan Investment Policy Statement and requirements within each investment program's respective investment policy statements. The Executive Committee determines the necessary investment actions to meet the cash needs and coordinates with other Investment Department personnel accordingly. This process occurs proactively, well in advance of the cash needs, typically about 6 weeks, if not more.

The Model can also be used to simulate asset reallocations within the Total Fund portfolio that do not involve cash.

Forecasting Operational Cash Needs

Since the early 2000s, the non-investment income inflows into Trust Cash Held with the State Treasurer, predominantly from the receipt of employer and member contributions, have consistently been insufficient to cover VRS' monthly benefit payments and administrative and

personnel expenses. This is not uncommon for mature plans. Therefore, VRS' operational cash flows must be monitored and transfers made to ensure sufficient funds are in place to meet operational cash needs. Typically, five to seven business days prior to month end, VRS' Chief Financial Officer (CFO) will begin the process of projecting the upcoming month's expenses that need to be paid to identify and confirm cash needs and provide time to transfer cash to meet these needs.

Cash Available to Fund Payments

Before assessing cash needs, the CFO will determine the current cash available within the accounts held by the Treasurer of Virginia, including the current balance of VRS' LGIP account. Any cash available in the LGIP to pay expenses will remain invested until it is needed to cover payments to maximize the investment returns for the Trust.

Cash Needed to Fund Payments

To estimate monthly benefit payments, the CFO determines the projected gross retirement payments, non-recurring payments (such as refunds), partial lump-sum option payments and third-party payments for long-term disability benefits. These are determined through VNAV and VRS general ledger data. Additionally, the CFO factors in the monthly outflow associated with the current fiscal year's appropriated operating budget, calculated as 1/12 of the total budget.

Calculation of Cash Shortfall

Subtracting the cash needed to fund payments from the cash available to fund payments reveals the cash shortfall to be funded. VRS works to ensure a cash buffer of approximately \$50 million will remain as Trust Cash held with the State Treasurer. The CFO will then request a cash transfer from the Investment Department which is communicated through email to members of the Investment Department, Investment Accounting Department, Finance Department and State Treasurer.

Sourcing the Cash Shortfall

As previously noted, the Investment Department typically sources cash from the BNYM VRS Cash account to fund the transfer request. Consistent with the cash transfer process, Investment Accounting will prepare a direction letter per the Investment Department's instructions. Once the direction letter is approved, BNYM will process the transfer and deposit the funds into the VRS Trust Cash held with the State Treasurer.

SCOPE AND METHODOLOGY

The primary purposes of our examination were to:

- Determine if cash management processes support operational needs and comply with applicable statutory requirements;
- Ascertain whether bank and investment accounts significant to cash management are adequately monitored; and
- Evaluate if cash deposits are reasonably protected in the event of bank failure.

GENERAL ASSESSMENT AND UNDERSTANDING

We obtained a general understanding of the Cash Management practices and related controls by meeting with key individuals across the organization and observing processes and systems. We also reviewed the *Code of Virginia*, applicable policies and procedures and other relevant documents.

CASH DEPOSITS

Statutory requirements for cash deposits and related investments were evaluated by confirming the applicable *Code of Virginia* sections with the Finance and Investment Departments and assessing them relative to processes performed by the State Treasurer and VRS.

Compilation of the Daily Asset Allocation report was evaluated through observation of Investment Department staff creating the report as well as a demonstration and discussion of any adjustments impacting the cash asset class. Data from the Daily Asset Allocation report was obtained for the entire audit period, with the weight of the cash asset class reviewed for compliance with the VRS Defined Benefit Plan Investment Policy Statement.

PROTECTION OF CASH DEPOSITS

Coverage provided by the FDIC and SPDA for Cash held with the State Treasurer and Master Custodian and VRS' role in submitting any related claims were assessed through discussion with

VRS executive management and review of FDIC and SPDA guidance to determine if deposits are reasonably protected in the event of bank failure.

Further, each bank account comprising Cash held with the State Treasurer was reviewed for SPDA coverage by looking up each account on the Department of Treasury's SPDA Account Balance Search website.

CASH TRANSFERS

All VRS monthly cash sweep vouchers were selected for review to determine if they were appropriately authorized, completed timely, accurately recorded in the VRS general ledger and in agreement with supporting documentation.

All cash transfers from the Master Custodian to the State Treasurer to fund monthly benefit payments were selected for review to determine if the transactions were appropriately authorized, accurately recorded in both the VRS general ledger and BNYM's records and in agreement with supporting documentation.

CASH MANAGEMENT

Access listings for all bank accounts with the State Treasury, the VRS LGIP account and the Cash Database were obtained and reviewed for the principle of least privilege and appropriateness in relation to each user's job responsibilities.

All compliance rules in the portfolio management software applied to the BNYM VRS Cash and Rebalance accounts were obtained and reviewed for agreement with the applicable Investment Policy Statements. Monitoring of best execution and portfolio risk analyses were discussed with Investment Department staff to determine if they support compliance with the Investment Policy Statements.

All portfolio oversight checklists for the STIF account were obtained and reviewed for monitoring for requirements included in the Investment Advisory Agreement. A summary of the most recent annual due diligence meeting was obtained to review for evidence of additional monitoring of the account and VRS' relationship with the investment manager.

All monthly performance reports for the BNYM VRS Cash, BNYM VRS Rebalance and STIF accounts were obtained to confirm proper approval by the designated Investment Department staff.

CASH RELATED RECONCILIATIONS

All monthly reconciliations for bank accounts holding Trust Cash with the State Treasurer were selected for review to determine if they agreed to supporting documentation, were completed timely and were properly reviewed.

All monthly reconciliations for the BNYM VRS Cash and BNYM VRS Rebalance accounts were selected for review to assess whether they agreed to supporting documentation, were completed timely and were properly reviewed. Additionally, reconciliations prepared as of quarter end were reviewed to determine if they were submitted timely to and reviewed by the Investment Accounting Department.

The quarterly reconciliation for the STIF account was selected for review to evaluate if it agreed to supporting documentation and was submitted timely to and reviewed by the Investment Accounting Department.

CASH FORECASTING

All monthly forecasts for operational cash needs were selected for review to determine the reasonableness of inputs for the estimation process.

Data entry, data review and report generation for the Cash Database were evaluated through observation of Investment Operations staff performing daily update activities to determine if the processes supported data quality and cash forecasting needs.

Monitoring and analysis processes for the VRS Rebal Global Model were assessed through observation of the Investment Department staff performing their daily update and review processes to determine if they support cash forecasting needs.

CONCLUSIONS

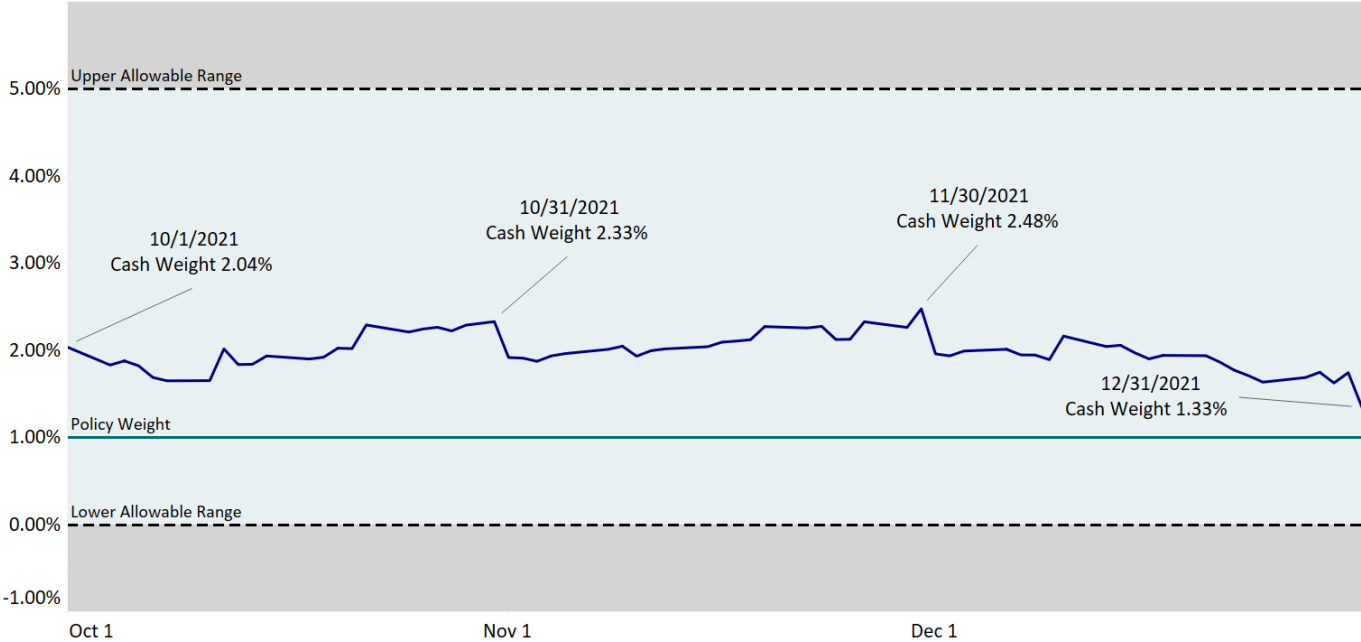
GENERAL ASSESSMENT AND UNDERSTANDING

Our review found that cash management processes support operational needs and comply with applicable statutory requirements, bank and investment accounts significant to cash management are adequately monitored and cash deposits are reasonably protected in the event of bank failure.

CASH DEPOSITS

Processes performed by the State Treasurer and VRS support compliance with statutory requirements applicable to cash deposits and related investments. The Investment Department's compilation of the Daily Asset Allocation report includes appropriate review processes and incorporation of adjustments into the report. VRS' data and reporting supports management of the cash asset class in compliance with the VRS Defined Benefit Plan Investment Policy Statement, as reflected below.

Cash Asset Allocation over Audit Period



Sources: BNYM accounting data and adjustments provided by Investment Department staff

PROTECTION OF CASH DEPOSITS

Discussion with VRS executive management regarding FDIC and SPDA coverage and VRS' role in the claims process and review of the related guidance indicated that Cash held with the State Treasurer and Master Custodian is reasonably protected in the event of bank failure. Further, each bank account comprising cash held with the State Treasurer was located in the Department of Treasury's SPDA Account Balance Search website indicating SPDA coverage.

CASH TRANSFERS

Cash transfers from the Master Custodian to the State Treasurer to fund monthly benefit payments were appropriately authorized, accurately recorded in both the VRS general ledger and BNYM's records and agreed with supporting documentation. VRS monthly cash sweep vouchers were appropriately authorized, completed timely, accurately recorded in the VRS general ledger and in agreement with supporting documentation.

CASH MANAGEMENT

All compliance rules in the portfolio management software for the BNYM VRS Cash and Rebalance accounts agreed with the applicable Investment Policy Statements. Discussion with Investment Department staff for the monitoring of best execution and portfolio risk analyses indicated compliance with the Investment Policy Statements for both accounts.

Review of the portfolio oversight checklists for the STIF account demonstrated monitoring for requirements included in the Investment Advisory Agreement. Review of the summary of the most recent annual due diligence meeting indicated additional monitoring of the account and VRS' relationship with the investment manager.

The monthly performance reports for the BNYM VRS Cash, BNYM VRS Rebalance and STIF accounts were reviewed and properly approved by the designated Investment Department staff.

Access reviewed for all bank accounts with the State Treasury, the VRS LGIP account and the Cash Database support the principle of least privilege and was appropriate based on each user's job responsibilities.

CASH RELATED RECONCILIATIONS

The monthly reconciliations for bank accounts holding trust cash at the Treasurer and BNYM were completed timely, properly reviewed and in agreement with supporting documentation. Reconciliations prepared as of quarter end were submitted to and reviewed timely by the Investment Accounting Department in accordance with VRS policy and procedures.

The quarterly reconciliation for the STIF account agreed with supporting documentation and was submitted to and reviewed timely by the Investment Accounting Department.

CASH FORECASTING

The review of inputs into the monthly forecasts for operational cash needs were determined to be reasonable for the estimation process.

The processes over Investment Operations staff's data entry and review of the Cash Database and report generation practices from the Cash Database ensure the data quality necessary to support VRS' cash forecasting needs.

Likewise, the Investment Department staff's daily update and review processes for the VRS Rebal Global Model provide monitoring and analysis necessary to support VRS' cash forecasting needs.

FOLLOW-UP ON PRIOR REPORTS

There were no outstanding audit recommendations to consider.

RECOMMENDATIONS

We have no written recommendations to offer as a result of our review.

MANAGEMENT EXIT CONFERENCE

This report was distributed to Ms. Bishop, Mr. Schmitz, and other members of VRS' management and staff for review and comment. They expressed substantial agreement with this report.

Cash Management Pg. 27 of 28

REPORT DISTRIBUTION

Submitted to the Audit and Compliance Committee at its meeting held
June 16, 2022.

MEMBERS OF THE AUDIT AND COMPLIANCE COMMITTEE

Joseph W. Montgomery, Committee Chair, Board Vice Chair
W. Brett Hayes, Committee Vice Chair
A. Scott Andrews, Board Chair

WITH COPIES TO:

OTHER MEMBERS OF THE BOARD OF TRUSTEES

J. Brandon Bell, II
John M. Bennett
Michael P. Disharoon
William A. Garrett
Susan T. Gooden
Troilen G. Seward

VRS EXECUTIVE LEADERSHIP

Patricia S. Bishop
Ronald D. Schmitz

Members of the Director's
Executive Committee

AUDITOR OF PUBLIC ACCOUNTS

Staci Henshaw

JLARC

Kimberly A. Sarte
Jamie Bitz

PRINCIPAL AUDITOR IN-CHARGE

Kristy M. Scott, CPA, CISA, CIA

AUDIT SUPERVISOR

Judy Bolt, CPA, CIA, CISA, CFE

Review of IT General Controls

As of October 1, 2021

Highlighting VRS Core Values: *Integrity, Teamwork, Accountability* and *Agility* in Action

THIS REPORT IS INTENDED SOLELY FOR THE USE OF THE VRS BOARD OF TRUSTEES AND THE MANAGEMENT OF VRS AND IS NOT INTENDED FOR OTHER PURPOSES.



TABLE OF CONTENTS

TITLE PAGE	1
TRANSMITTAL LETTER	2
EXECUTIVE SUMMARY	3
BACKGROUND	4
SCOPE AND METHODOLOGY	15
CONCLUSIONS	22
FOLLOW-UP ON PRIOR REPORTS	30
RECOMMENDATIONS	31
MANAGEMENT EXIT CONFERENCE	35
REPORT DISTRIBUTION	36
PRINCIPAL AUDITOR IN-CHARGE	36

Dear Members of the Audit and Compliance Committee,

We have completed audit number 444, “Review of the IT General Controls” The main purpose of our audit was to assess the overall effectiveness and security of the IT architecture within VRS. This examination assessed VRS’ performance against its own IT Security Standards which incorporates mandatory Virginia Information Technologies Agency (VITA) governance requirements. VITA governance is designed to provide an operating environment that reasonably minimizes the risk associated with IT processing.

We conducted our audit in accordance with the *International Standards for the Professional Practice of Internal Auditing*. These standards require that we plan and perform the audit to obtain sufficient and appropriate evidence to provide a reasonable basis for the conclusions based upon our audit objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

This report was distributed to the VRS Director and members of management for review and comment. Management expressed substantial agreement with our report and will issue a written response to the recommendations contained in this report.

We appreciate the cooperation and assistance of the Information Technology Department throughout this audit.

Respectfully Submitted,

A handwritten signature in black ink that reads 'Jennifer P. Bell Schreck'.

Jennifer P. Bell Schreck, CPA, CISA, PMP
Audit Director

EXECUTIVE SUMMARY

We conducted an examination of VRS' IT General Controls as of October 1, 2021 which focused on general controls which apply to all systems, components, processes and data within VRS' internal Information Technology (IT) environment. These basic controls are applied to IT systems to protect the integrity of the data and processes the systems support. For the purposes of this examination, we focused largely on VRS' compliance with general controls set forth in the VRS Security Policy, User IT Security Policy and VRS Security Standard. Specifically, our review determined:

- IT governance framework is established to protect VRS' systems and IT environment;
- Known threats are managed and protected, along with the development of comprehensive response plans for evaluating, managing and reporting security incidents;
- Regular monitoring is occurring to ensure protection processes continue to function as intended and new vulnerabilities are identified and mitigated;
- Data protection mechanisms are in place to guard IT operations from outside threats including transmission integrity outside VRS boundaries;
- IT inventory is being managed and disposal of antiquated equipment is performed without data disclosure; and,
- Externally managed facilities' audit reports are reviewed and assessed regularly in light of the VRS IT security environment.

Application controls supporting specific applications were not addressed as they are reviewed in separate engagements (See reports [No. 417](#) and Report [No. 440](#)). VRS' Policies and Standards conformance with VITA's Security Program are not addressed as they are reviewed in a separate annual engagement the results of which were most recently shared in Report [No. 442](#).

We include four formal opportunities for improvement in this report surrounding the need to:

- Ensure completion of required Continuity Plan testing, training exercises and review;
- Improve processes to regularly update configuration and procedural documentation;
- Fortify processes surrounding devices used for international travel; and,
- Enhance the data fix processes and controls.

We discuss these areas in more detail within the Recommendations section of the report.

SNAPSHOT

Systems within VRS' IT environment rely on **general controls** which are put in place to ensure **confidentiality, integrity** and **availability** of the data and processes within the environment.

VRS routinely **performs risk assessments** and **business impact analysis** to support the **design** of the general controls within its **IT control environment**.

As of the **October 2021**, VRS' **critical systems** were available **99.94%** of the **time** during planned availability windows.

AUDIT ASSESSMENT

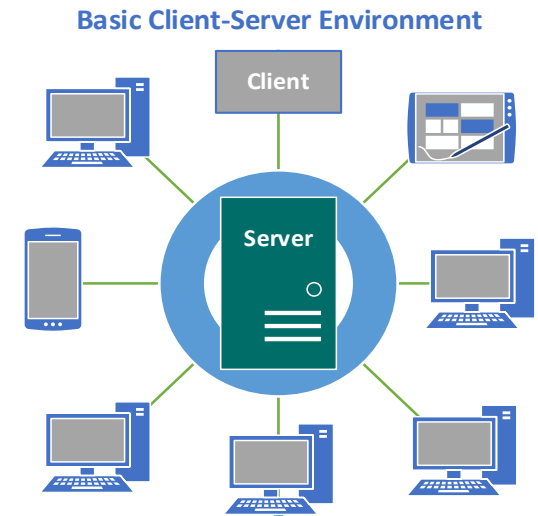
Overall, the General Controls surrounding IT processing and the environment are well designed and functioning properly to reasonably minimize the risks associated to an adequate residual level.

Written Recommendations: 4

BACKGROUND

INTRODUCTION

The foundation of VRS' Information Technology (IT) environment is designed with a client-server architecture. A client-server model is a modern networking architecture that divides system processing between local clients and central servers to better employ available computing resources and share data processing power. A server, in this environment, is a piece of hardware that provides specific services to users and can provide a large number of these services to multiple users simultaneously. The client is typically the user's standalone computer, tablet or mobile device which requests resources from the server through an interface. There are many advantages of this environment over a mainframe environment; however, an important advantage of the client-server architecture is centralized data protection with access controls that are enforced by implemented security policies.



To protect these types of environments, general controls are the foundation to ensure the integrity of the data and completeness and accuracy of the processes performed within the environment. These controls pertain to all systems, components, processes and data which reside within the client-server environment. The related application controls which protect the integrity of the input, processing and output of specific applications were excluded from this review and are evaluated separately as discussed in the scope section below.

IT GOVERNANCE

IT governance encompasses the roles, responsibilities and processes that ensure the efficient and effective use of IT in enabling VRS to achieve its goals. IT governance provides the structure that links IT processes, IT resources and information to agency strategies and objectives. VRS has established an IT Security Program to implement and maintain its business and technology

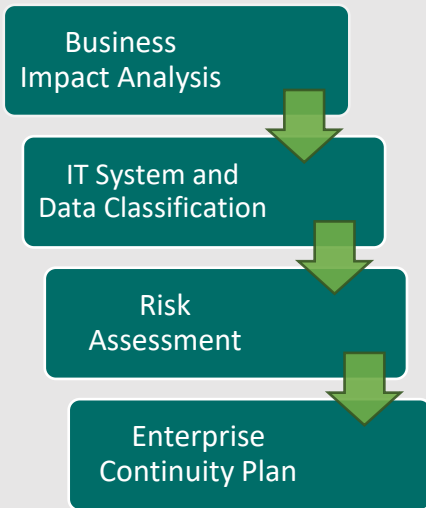
Appropriate **general controls** must be in place **before** **reliance** can be placed upon **application controls**.

environment and to ensure compliance with applicable Commonwealth requirements. At the commencement of the review, VRS had documented the governance of its IT Security Program in the VRS Security Policy, User IT Security Policy and VRS Security Standard which governed the management of these processes.

Note, after the audit period, VRS revised and approved a new security governance document called the VRS Information Security Program Policy (ISPP) which replaced the VRS Security Policy and VRS Security Standard.

BUSINESS CONTINUITY PLAN CREATION

Each exercise **feeds** off the other to **create** a holistic and effective **continuity plan**.



BUSINESS CONTINUITY

Business continuity planning provides a proactive means to understand the operating and IT control environment and mitigate and recover from risk incidents which disrupt business operations. This type of planning deals with the safety of personnel and restoration of critical locations and operational processes, including IT, after a disaster or emergency situation occurs.

VRS' business continuity plan is referred to as the VRS Enterprise Continuity Plan. The creation of an effective and comprehensive continuity plan is a multi-step serial process which involves the creation of fundamental components to assist in the development of a holistic overarching plan. The foundational elements of the continuity plan include the following three components: a Business Impact Analysis (BIA), an IT System and Data Sensitivity Classification and a Risk Assessment (RA).

VRS is required to create business continuity documentation, train appropriate personnel in continuity procedures and test recovery procedures regularly. Once the BIA, IT System and Data Classification, RA and Enterprise Continuity Plan are created, annual reviews and updates of these documents are required per the VRS Security Standard sections 3, 6 and CP-2 and the [VITA Risk Management Standard](#). Then every three years, a full revision of the RA and BIA is required per the VRS Security Standard sections 3 and 6 and the [VITA Risk Management Standard](#).

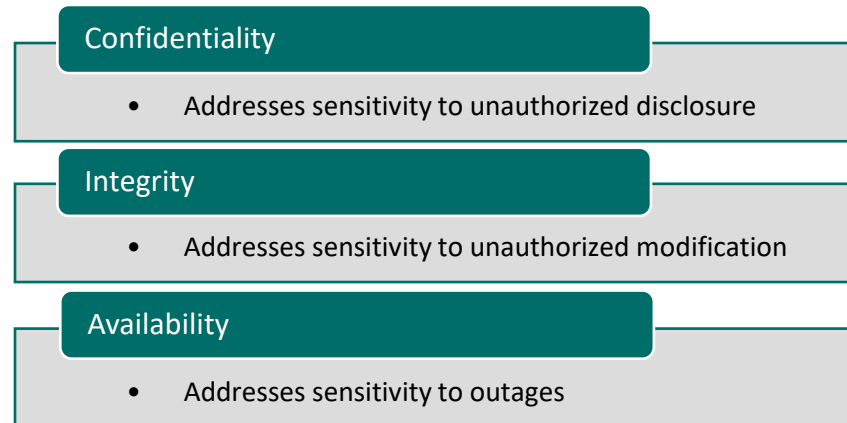
Business Impact Analysis

The BIA is a critical organizational tool that facilitates the process of gathering and identifying business functions essential to the mission of VRS. The BIA establishes the basis for other contingency management pieces, as it identifies, prioritizes and maps resources to VRS business processes.

Identifying and evaluating how a disaster may impact VRS business provides a basis for implementing recovery strategies that consider critical business functions and prioritize how VRS should invest in prevention and recovery strategies to mitigate the impact of a disaster on those functions. The information created from this analysis becomes the primary input into the IT System and Data Sensitivity Classification.

IT System and Data Classifications

The IT System and Data Sensitivity Classification process is used to identify and classify all VRS IT systems and data according to sensitivity with respect to:



Data Sensitivity is **directly proportional** to the **material** impact of a **compromise** of the **data** with respect to data **sensitivity criteria**.

Sensitive data is any data for which compromise with respect to confidentiality, integrity and/or availability could have a material adverse effect on VRS' mission or the privacy to which its members and beneficiaries are entitled. Sensitivity classification is based on the most sensitive data that the IT system stores, processes or transmits. Once this classification is complete, it allows VRS to focus resources on the highest risk or most sensitive systems based on severity. The information captured in this classification documentation becomes the primary input into the Risk Assessment.

Risk Assessment

The RA process identifies and analyzes the business risks that may affect VRS' ability to complete its mission. VRS' risk assessment focuses on the appraisal of the risk level of IT systems identified as sensitive by:

The **Enterprise Continuity Plan** is not an IT Plan, rather it is a **business** plan through which VRS shows its **TEAMWORK** across departmental and organizational boundaries to **respond** and **restore critical business processes** based off a specific **disturbance** to the organization.

- Identifying potential threats to the IT system and the environment in which it operates;
- Determining the likelihood that threats will materialize;
- Identifying and evaluating vulnerabilities; and,
- Determining the loss impact if one or more vulnerabilities are exploited by a potential threat.

Once completed, the RA provides the final building block prior to the creation of the Enterprise Continuity Plan and the more detailed IT Disaster Recovery Plan (DRP) that support and guide personnel in the recovery of business operations.

Enterprise Continuity Plan

VRS' continuity plan provides the framework for restoring essential business functions in the event of an emergency that affects operations and enables VRS to maintain or recover service within an acceptable, pre-defined time period. The plan's objectives are to:

- Ensure that VRS can perform its core business processes within established recovery time objectives for a period of up to 30 days or until normal operations can be resumed;
- Reduce or mitigate disruptions to operations;
- Minimize damage and loss to property, records, systems and equipment;
- Achieve VRS' timely and orderly recovery and reconstitution from a continuity event;
- Ensure and validate continuity readiness through a dynamic and integrated continuity testing, training and exercising program; and,
- Ensure that the program is updated as necessary to maintain recovery capabilities reflective of the current business environment.

Part of the continuity plan, but broken out separately, is the IT DRP which provides a comprehensive statement of procedures or actions to be used during and after an emergency or disruptive event. The objective of these detailed procedures is to bring back up essential IT functions and provide the business the ability to perform their duties within VRS' defined recovery time and eventually return to normal operations, when possible.

Enterprise Continuity Plan Testing and Training

The training of responsible personnel and testing of the continuity plan are vital to ensure that plans are sufficiently defined and documented and executable within the identified tolerances. Per the VRS Security Standard CP-3, VRS must train applicable users in their business continuity roles and responsibilities within 30 days of assuming a role or responsibilities or when required by information system changes, and annually thereafter.

Additionally, CP-4 requires that VRS tests its contingency plan on annual basis or more frequently if required to address an environment change, by using approved tests to determine the effectiveness of the plan and the organizational readiness to execute the plan. After the tests have occurred, results of the exercises should be analyzed and lessons learned or identified corrective actions to the plan should be implemented, if necessary.

USER SECURITY AWARENESS

A critical feature of a security program and an organization's IT governance is a user's security understanding and awareness of the information system environment.

Security Awareness Training

One of the best practices of a strong security program is the regular reinforcement of security practices and the organization's IT policy. VRS performs this through onboarding and annual mandatory security awareness training for all personnel, including contractors. The course is provided online through VRS' training and development application.

Regular reiteration of security best practices keeps personnel up to date with the evolving information technology landscape, including new IT trends. Due to this, VRS provides its technology users additional security training on focused topics throughout the year to highlight new or emerging IT practices and trends which may impact VRS. This training is offered through numerous channels, from screensaver messaging to Netflix quality short videos to "VRS Today" meetings.

VRS also exposes VRS technology users to real-world situations by carrying out monthly phishing exercises to reinforce concepts delivered through security training sessions. For users who are unsuccessful in these exercises, VRS reiterates the appropriate response through additional training to help impact those user's future decisions when presented with risky scenarios.

Review of IT General Controls Pg. 8 of 36

**TECHNOLOGY ACCESS
STANDARD FOR STAFF WITH
ELEVATED PRIVILEGES**

We **commend** VRS for the **creation** of this governance document which **reinforces** VRS' culture of **ACCOUNTABILITY** and **INTEGRITY** and outlines the **expected behavior** for individuals who are granted these **responsibilities**.

At a policy level, these VRS practices conform to the VRS Security Standard AT-2 which states that VRS must provide basic security training to all information system users (employees and contractors) annually or more often thereafter.

Role-Based Training

VRS directs role-based security training to be provided to personnel with assigned security roles and responsibilities before authorizing access to the system or performing assigned duties as dictated by AT-3 in the VRS Security Standard. Additionally, the VRS Security Standard AT-2-COV requires the Agency Head to receive role-based training related to the position responsibilities and requirements of the Commonwealth's information security program.

Beyond these requirements, VRS has established an IT code of ethics referred to as the "Technology Access Standard for Staff with Elevated Privileges". This Standard outlines VRS' expectations of trust, *accountability* and conduct to which staff will adhere to act in a professional and secure manner to preserve the sensitive nature of VRS' systems and information. For individuals with enhanced privilege roles, this Standard is reaffirmed and signed annually.

DATA PROTECTION

Sensitive data is information which, if compromised with respect to confidentiality, integrity, or availability, could adversely affect VRS' mission or the privacy to which members or retirees are entitled. VRS takes its *accountability* and responsibilities to protect its data very seriously.

Data is classified as sensitive if its compromise results in a material and significant adverse effect on VRS interests; the inability of VRS to conduct its business; or a breach of stakeholder privacy expectations. VRS documents and characterizes the types of data managed and identifies sensitive data and sensitive IT systems classifications within its RA and IT system and data classification processes.

VRS protects data by converting or encrypting the stored or transferred information into a form that is unreadable to an unauthorized user or process. Encryption tools can prevent unauthorized disclosure of information and detect changes to information during transmission. Encrypted data must be converted back to a readable form prior to use. Authorized users are able to decrypt this data seamlessly through use of an encryption key. Further, VRS encrypts data which is transferred from its business partners and employers to ensure that the data is protected during transit. This

encryption helps ensure that any information that has been misdirected, intercepted or otherwise obtained will be extremely difficult to compromise.

Additionally, VRS users have access to sensitive information as part of their normal job responsibilities. These users are expected to safeguard information and may not disclose or share this information except in accordance with approved business processes. VRS users are prohibited from copying sensitive information from any VRS network to any other technology storage media unless the data is encrypted and there is a written exception approved by the VRS Director. This includes storage of such sensitive data locally on VRS laptops.

RANSOMWARE CONTROLS

Ransomware is a type of malicious software designed to **block access** to a computer system until a ransom is paid.

A complete, tested and unconnected **backup** is one **mitigation** technique to **thwart** a successful take-over of a computer system and **facilitates restoration** of the infected system in a **reasonable** amount of **time**.

INFORMATION SYSTEM BACKUPS

Data loss comes in many forms; however, regardless of the event causing the loss, strong backup plans are necessary to ensure systems can be restored to their previous condition. To safeguard its data and support the continuity of operations, VRS performs routine and regular backups of its systems to allow for restoration of these systems at any given time. As an additional layer of protection, per the VRS Security Standard CP-9-COV and MP-4-COV, VRS secures backup media off-site in an encrypted form. Additionally, VRS has a hot site or an alternate processing site established to allow VRS systems and personnel to transition to if a significant disruption impacts VRS' ability to perform normal processing at the primary site.

CHANGE MANAGEMENT

VRS' change management process includes a series of steps and controls that govern the implementation of changes to its production network. Change management involves the systematic proposal, justification, implementation, testing, review and disposition of changes to the systems, including system upgrades and modifications. Adequate controls over modifications to systems prevent unauthorized or potentially inaccurate changes from being incorporated into the production environment. VRS personnel protect and maintain the *integrity* of VRS applications and business processes by performing effective and controlled change management processes.

Patch Management

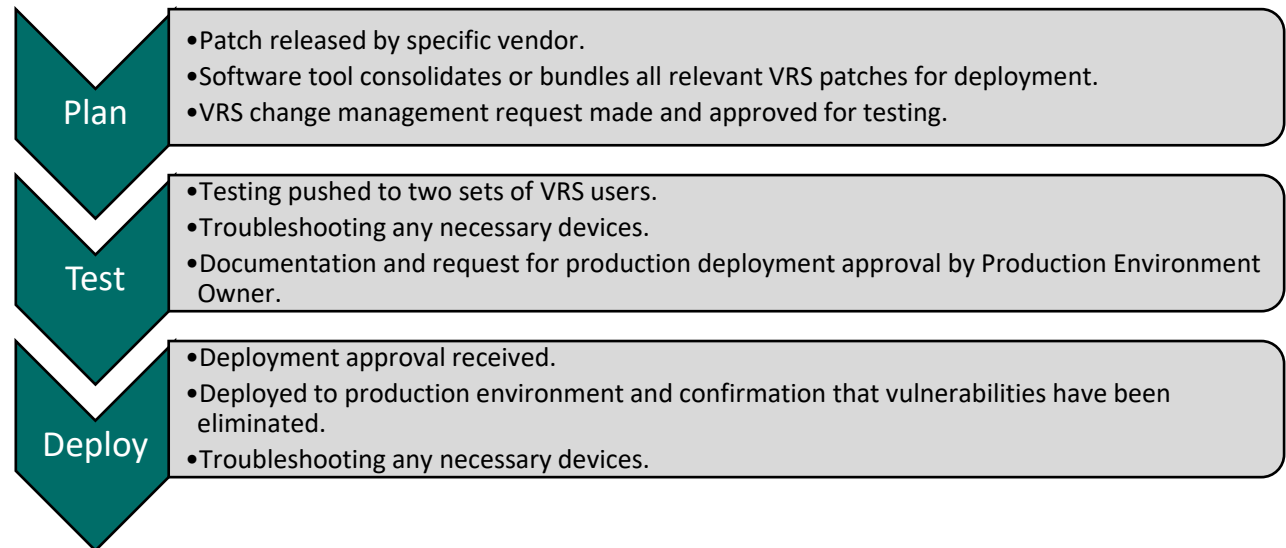
A subset of the change management process is patch management. This is the process of installing patches on existing operating systems, applications and software tools within the IT environment. Patches enable systems to stay up-to-date and secure and are usually released by software and

hardware vendors to address specific security concerns and functionality of programs. VRS has regular processes in place to identify, test and implement patches in the VRS environment timely. All patching activities follow the standard change management process reflected below prior to being implemented into the production environment.

VRS uses a software tool to continuously scan the VRS network looking for vulnerabilities. This tool provides VRS staff with a dashboard of vulnerabilities, rated based on severity. In practice VRS works to have all patches implemented within 30 days of the vulnerability being identified. Lower rated vulnerabilities and patches are consolidated for monthly deployment to all devices as described below. Critical vulnerabilities move through the processes immediately and are implemented as soon as possible.

This approach exceeds the requirement specified in the VRS Security Standard RA-5 which states patches should be addressed within 90 days of identification.

Monthly Patching Process



Monthly patches, once consolidated, are systematically tested, approved and ultimately deployed, which takes approximately one week. VRS has two sets of testers which are used to ensure that the patch package does not break the functionality or disable the device; however, not all patches are

created equally. VRS personnel show their *agility* by troubleshooting devices and working with the vendor, if necessary, when patching issues are identified.

Once successfully tested, documentation is kept and presented through the change management process to appropriate IT managers for approval. Upon approval, the patches are pushed to the rest of the agency. After deployed to the entire agency, VRS confirms deployment with the network scanning tool to ensure the identified vulnerability or vulnerabilities have been mitigated.

Data Fix Process

VRS uses a tool to make data corrections through its data fix process. This is a last resort method of correction, which provides an adjustment mechanism to records within VNAV when there is no routine way to make the change through the application. The nature of these adjustments varies based on the business need.

ASSET MANAGEMENT

IT Asset Management is the practice that involves maintaining an accurate hardware and software inventory and tracking licensing use. VRS' understanding of which hardware and software assets are deployed throughout the IT environment helps to optimize the use and maintenance of its assets.

Asset and License Inventory

VRS uses a software tool to track and monitor all VRS hardware and software assets and location in real-time. On demand as needed, VRS can perform a review of all devices, a specific subset of devices, or one specific device to determine hardware needs and availability. To supplement its virtual monitoring, VRS annually performs a full physical inventory of all devices throughout VRS to account for the location and ensure that devices are still available to the business.

Further, the same inventory tool is able to manage licensing tracking and software monitoring throughout VRS on all IT devices. VRS personnel demonstrate the organization's *integrity* by monitoring the use of software products to ensure compliance with all licensing agreements. The use of this tool also provides VRS increased visibility into the organization's resources and needs to allow for more effective business decisions and solutions.

Portable Storage Devices

VRS distributes portable storage devices to VRS personnel who have responsibilities to transfer documentation for a business purpose. These devices are not used to transfer information to or from VRS sensitive systems. Portable storage devices are scanned upon attachment to the VRS owned device to protect the VRS network and devices from infection.

Prohibited Services, Hardware and Software

Particular vendors have been identified by the federal government which convey a high risk of use, and the Commonwealth has aligned this prohibition under [VITA's Prohibited Hardware, Software and Services Policy](#). This policy is mandatory and lists the specific vendors with which VRS is prohibited from entering into, extending or renewing a contract. VRS has a responsibility to manage its use of services, hardware and software within the restrictions of this policy and uses its asset and license inventory software tool to support this.

Asset Disposal

When inventory is no longer needed or becomes obsolete, VRS must dispose of it while protecting and removing any data which may still be accessible on the device. The VRS Security Standard MP-6 states that VRS must sanitize information system media prior to disposal and must employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

To ensure proper disposal, VRS follows VITA's mandatory [Removal of Commonwealth Data from Surplus Computer Hard Drives and Electronic Media Standard](#). This standard lays out the holistic framework for proper removal and disposal of electronic media at the earliest time after being taken out of use and not later than 60 days.

Use of Unsupported Systems

As of our audit period, VRS had a decentralized process in place to track implemented systems support longevity within the specified area's purview. It is common practice for a developer, vendor or manufacturer to give customers plenty of notice prior to the termination of support of their system or related components. Once this is announced, VRS strives to replace any equipment prior to such date because these unsupported components become increasingly vulnerable over time and could provide substantial opportunity for a bad actor to exploit weaknesses present in the unsupported installed components.

THREAT MANAGEMENT

Threat management uses a combination of early detection systems such as intrusion prevention systems, firewalls and security tools to proactively monitor for and counter threats to a network. VRS has put in place various threat management techniques to ensure the safety and security of the VRS network and its associated processes. Examples include firewalls and intrusion detection systems devices to record and block improper and malicious traffic from entering the network. Once traffic enters the network, VRS uses monitoring and logging of all activity to reduce the impact of risks to VRS' IT systems and data.

VRS configures all IT systems capable of logging to ensure that there is a record of activity. All events are logged into a central system. Events are correlated through the use of intrusion detection or prevention systems. Such IT security logging and monitoring allows VRS to capture data regarding events that appear innocent in isolation but when viewed as part of a pattern can be determined to be malicious. Unexplainable activity is reported to the System Administrator for diagnosis.

VRS takes a proactive security approach to anticipate potential situations that could lead to losses or risks which could exploit its environmental context. VRS actively performs vulnerability assessments at least once a quarter and performs penetration testing at least annually or when an environmental change has occurred. Further, VRS IT Security investigates and responds to potential security incidents occurring with VRS IT assets. Additionally, VRS has contracted with a third party to perform and support VRS security threat management and monitoring services, 24 hours a day, 7 days a week, 365 days a year.

Externally Managed Facilities

Beyond VRS' office buildings, VRS has contracted for two external data centers which are owned by a private entity. These data centers have physical and environmental controls in place to protect the assets of VRS and other clients. These controls are assessed by a third party through a SSAE 18 report which is reviewed by VRS IT security personnel in light of the VRS IT security environment and any impacts to it based on the report results. Specifically, VRS has established a process to monitor and regularly review each released SSAE 18 report for any associated IT third party to ensure that any unresolved weaknesses noted in these reports are identified and compensating controls are put in place to ensure the integrity of VRS assets.

VRS also monitors access to these facilities by authorized personnel through the vendor's online badge reporting system which allows VRS to review all badge access to VRS' area or equipment.

Incident Response Plan and Mandatory Breach Notifications

VRS has an Incident Response Plan (IRP) for evaluating and reporting potential security incidents and weaknesses. This framework lays out a prescriptive set of processes and procedures to ensure information security events and weaknesses associated with information systems are communicated in a manner which allows timely corrective action to be taken. These processes also ensure VRS' compliance with the *Code of Virginia* in regard to mandatory breach notifications to affected parties.

SCOPE AND METHODOLOGY

The primary purpose of this examination was to determine the adequacy and effectiveness of key general controls over the systems housed in VRS' IT environment. In support of this purpose, the following objectives were established.

- Determine if an IT governance framework is established to protect VRS' systems and IT environment;
- Assess whether known threats are managed and protected, along with the development of comprehensive response plans for evaluating, managing and reporting security incidents;
- Evaluate whether regular monitoring is occurring to ensure protection processes continue to function as intended and new vulnerabilities are identified and mitigated;
- Ensure VRS has established data protection mechanisms to guard IT operations from outside threats including transmission integrity outside VRS boundaries;
- Assess whether IT inventory is being managed and disposal of antiquated equipment is performed without data disclosure; and,
- Ensure that externally managed facilities' audit reports are reviewed and assessed regularly in consideration in light of the VRS IT security environment.

COVERAGE OVER ADDITIONAL GENERAL CONTROLS

Logical Access, RAMS and **Physical Access** including **facilities security** will be reviewed in the new **Logical and Physical Access Examination** in the near future, which is further **supplemented** by **procedures** within program specific **projects** performed throughout Internal Audit's **Long-Range Plan**.

GENERAL ASSESSMENT AND UNDERSTANDING

We obtained a general understanding of VRS' general controls in the IT environment by reviewing applicable policies, procedures and other relevant governance and control documentation. We held meetings to discuss processes and controls with relevant personnel, as necessary. Finally, we validated key general controls were functioning as stated and intended.

IT GOVERNANCE

During our most recent review of VRS' Conformance with VITA Security Program ([Report No. 442](#)), we reviewed policies and standards around the IT environment as a whole to determine if VRS had appropriate governance and documentation. Further, we determined whether the VRS Security Policy and underlining VRS Security Standards have been approved by the VRS Director.

This examination builds on the preceding review's foundational governance elements by examining the detailed VRS processes, procedures and configuration guides in place which sufficiently meet overarching policy requirements, while confirming established controls are in place and the existence and validation of reasonable results.

BUSINESS CONTINUITY

We reviewed VRS' Enterprise Business Continuity Plan to determine whether a strong and repeatable plan was in place to recover essential business processes timely in the event of a significant business disruption. Along with the Enterprise Continuity Plan, we reviewed the underlying foundational documentation which includes the BIA, the IT system and data classifications and the RA which were developed to create and support this plan.

We assessed whether VRS had completed these foundational documentation activities in full, included all systems and were in compliance with the VRS Security Standard and [VITA Risk Management Standard](#), and determined whether reasonable approaches were taken in regard to relative known risks. We also evaluated whether this documentation was being regularly reviewed and updated to assure ongoing alignment with VRS' current business environment.

USER SECURITY AWARENESS

Security Awareness Training

We reviewed VRS' security awareness training course content for the most recent security awareness training provided to all VRS employees and contractors. We determined whether VRS' security awareness training course addressed the minimum criteria established in the VRS Security Standard AT-2-COV and [VITA's Cybersecurity Awareness Training Standard](#). We also considered whether this course was being provided timely to all new hires as they were onboarded and to all existing employees and contractors on an annual basis.

Role-Based Training

We reviewed VRS' role-based security training content for personnel with assigned security roles and responsibilities and for the Agency Head related to the position's requirements of the Commonwealth's information security program. We determined whether these role-based training courses addressed the minimum criteria established in the VRS Security Standard AT-2-COV and AT-3 and [VITA's Cybersecurity Awareness Training Standard](#).

DATA PROTECTION

We reviewed VRS' data protection policies and mechanisms to determine if they are adequately protecting systems information at rest and when transferred through cryptographic mechanisms. We also reviewed VRS incoming communications to assess whether they were appropriately limited to VRS recognized and defined authorized sources.

INFORMATION SYSTEM BACKUPS

We obtained and reviewed VRS' backup, storage and recovery policies and procedures for the IT environment to ensure all backup media is safeguarded appropriately. We determined the frequency of these backups were consistent with recovery time and point objectives documented in the Enterprise Continuity Plan, along with Library of Virginia retention schedules. We further determined whether files are encrypted and backups are stored offsite to protect confidentiality, integrity and availability. Finally, we evaluated who could perform backup processes and who had authorization to send and request files offsite.

PROCESSES EXCLUDED

Change management processes associated with the **System Development Life-Cycle** were **excluded** from this review.

These processes were **assessed**, as necessary, during recent **Internal Audit's Quarterly Reviews of Phase 4** of the **Modernization Program** and will be cycled back into regular engagements moving forward.

Actual backups of systems and its individual procedures, frequency of backups and regular validation of backups were not reviewed in this examination and will be included in future sensitive system application control examinations. Further, we exempted Library of Virginia retention schedules since they are currently under review by VRS and discussed further under the Follow-Up on Prior Reports section below.

CHANGE MANAGEMENT

The review of VRS' change management processes to determine if there was a formal, documented process for ensuring that only fully tested, reviewed and approved changes were incorporated into a system's production environment was reviewed most recently as a part of [Report No. 440](#) and therefore exempt from this review.

Patch Management

We reviewed VRS' patching processes for VRS workstations, servers and other assets. We discussed and performed a high-level walkthrough of the patching process with the responsible personnel to determine the actions that were occurring. We reviewed procedural documentation to confirm the items discussed were memorialized and change management approved practices were identified and included appropriate testing, review and approval prior to rolling them out to all devices. We reviewed the patching processes' documentation for the calendar year 2021, determining whether the new patches were installed within 90 days of the release of the patch as dictated in VRS Security Standard section SI-2. Once we confirmed these processes were occurring regularly, we judgmentally selected a few of the executed patches and assessed whether proper documentation, testing and approvals were present.

Data Fix Process

We reviewed the data fix process and procedures. We discussed and performed walkthroughs of the data fix process with the responsible personnel to determine the actions that were occurring. This included ensuring that personnel investigating data issues identified the proper cause prior to implementation to assess whether the issue was a symptom of another problem. We reviewed procedural documentation to confirm the items discussed were memorialized and change management approved practices were identified and included appropriate testing, review and approval prior to the implementation of the change. For the first nine months of 2021, we

judgmentally selected a sample of data fixes and evaluated whether proper documentation, testing and approvals were present.

ASSET MANAGEMENT

Asset and License Inventory

During the time of the examination, VRS was in the process of replacing the asset inventory tool prior to it reaching unsupported status in Spring 2022. This tool is the foundational element in the VRS asset inventory and software licensing management tracking. Initially, after discussion with management, we had planned to be involved and consult during the implementation of the new system and the establishment of the VRS processes for the management, distribution, tracking and security of VRS assets and software licensing agreements. However, during the engagement VRS suffered turnover in the management within this area, and any fieldwork surrounding these processes were subsequently delayed and exempted from this examination. Due to this, we will review the new tool's processes during an upcoming future examination.

Portable Storage Devices

We evaluated VRS' process and procedures surrounding authorization to use portable storage devices within the VRS environment. We assessed VRS processes for releasing and authorizing such devices into the VRS environment. Further, we evaluated whether VRS authorized only VRS-owned portable storage devices and prohibited the use of these storage devices on systems external to VRS. We determined whether VRS had implemented cryptographic mechanisms to protect the confidentiality and integrity of information stored on portable storage devices. Further, we ensured that VRS applies nondestructive sanitization techniques to portable storage devices prior to connecting devices to the VRS network as dictated in the VRS Security Standard section MP-6(3).

Prohibited Services, Hardware and Software

Finally, We validated VRS' compliance with [VITA's Prohibited Hardware, Software and Services Policy](#) which prohibits agencies from using or contracting for information technology services that are listed within it.

Asset Disposal

We obtained VRS' disposal policies and procedures to assess VRS employment of proper sanitization mechanisms with the strength and integrity commensurate with the classification of information

prior to the release of the asset and in accordance with [VITA's Removal of Commonwealth Data from Surplus Computer Hard Drives and Electronic Media Standard](#). We determined whether VRS tracks, approves and verifies media sanitization and disposal process actions. We reviewed the personnel and roles involved with disposing, validating and removing the equipment from VRS premises to assess the separation of duties to provide assurance that equipment was sanitized properly and was not disposed of prematurely. Further, we assessed VRS tests sanitization equipment at least on an annual basis to verify that intended sanitization is being achieved if the sanitization tool is used on sensitive systems.

Use of Unsupported Systems

We determined whether VRS uses any systems which are no longer supported by the developer, vendor or manufacturer as dictated in VRS Security Standard section SA-22. Once a system reaches unsupported status, it provides a substantial opportunity for adversaries to exploit new weaknesses present within the system. For any such system, we ensured VRS applied additional compensating controls and confirmed that management provided justification and retained documentation of the approval for the continued use of unsupported system components required to satisfy business needs.

THREAT MANAGEMENT

We determined the reasonableness of VRS' actions to protect IT operations from outside threats. We assessed if VRS had reasonable intrusion detection and prevention devices in place to protect VRS assets from unauthorized access, modification and deletion. We also evaluated whether VRS is protected against or limits the effects of denial-of-service attacks by employing security safeguards. We assessed VRS' use of spam and malicious code protection mechanisms at system entry and exit points to detect and eradicate unsolicited messages and malicious code. We reviewed how VRS protects system authenticity of communication and defends against the insertion of false information into communications. We also inquired whether VRS actively uses any open-source software. If in use, we then determined if VRS established appropriate compensating controls.

We sought assurance VRS has the ability to detect attacks and threat indicators through any type of connection to the network in accordance with VRS defined monitoring objectives. We reviewed the appropriateness of implemented internal and external traffic security monitoring and communication controls at the external boundary of the system and at key internal

boundaries. We further verified VRS appropriately limits the number of external network connections to each system. Finally, we assessed VRS monitoring practices around information disclosure through open-source information sites to ensure unauthorized information is not being disclosed.

Once we understood how VRS protected VRS assets, we evaluated VRS' proactive processes for identifying vulnerabilities. We confirmed VRS was performing regular vulnerability scans for public facing systems or when new vulnerabilities potentially affecting applications were identified or reported. Once these scans were completed, we assessed VRS' compliance with providing required quarterly summary reports of intrusion events to VITA Security. Further, we determined whether VRS conducted penetration testing at least on an annual basis as required by the VRS Security Standard section CA-8 along with the immediate remediation of any discovered weaknesses.

Finally, we obtained and reviewed the SSAE 18 report for VRS' external data centers to determine whether the physical and environmental internal controls are sufficiently robust and any weaknesses noted are compensated by VRS controls. We also evaluated VRS' process for reviewing these reports regularly to ensure the third parties continue to secure its environment appropriately; VRS is identifying and compensating for any vendor weaknesses that affect VRS; VRS considers and addresses any user entity controls included in the SSAE 18; and results are communicated to appropriate VRS senior management.

Incident Response Plan

We examined VRS response plans for reporting, evaluating and responding to potential security incidents referred to as the VRS IRP. We confirmed their adequacy to facilitate an efficient and effective response to information security incidents, limit the impact of said incidents and protect the confidentiality, integrity and availability of VRS information assets. We also reviewed plan compliance with minimum requirements defined in the VRS Security Standard.

We verified communication mechanisms were documented appropriately to allow for timely notifications between responsible personnel with incident response roles and responsibilities. We also determined whether personnel with these roles and responsibilities are trained on their assigned role within 30 days of assuming the role, when required by information system changes, and annually or more frequently as required by VRS Security Standard section IR-2. We

determined whether VRS was performing tests of the IRP at least annually to ensure plans continue to be adequately aligned with VRS current practices and procedures. Further, we assessed whether, once tests were completed, lessons learned were gathered from all participants and were incorporated into the plan appropriately.

Finally, we obtained the population of incidents occurring during the 2021 calendar year and planned to judgmentally select a few incidents for review to assess whether the plan was followed, proper documentation was retained and actions were taken based on the IRP during and after the incident.

CONCLUSIONS

GENERAL ASSESSMENT AND UNDERSTANDING

Our examination found the overall general control environment surrounding the IT systems reasonably minimizes risks associated with processing and the related IT assets at VRS. We found VRS' practices to be generally in compliance with the VRS Security Standard, and the controls in place address risks associated with areas of IT governance and associated operational controls surrounding data protection and threat management.

During the course of our examination, we did see certain areas where compliance with the VRS Security Standard could be improved which are discussed in the remaining sections of the report.

IT GOVERNANCE

VRS has created and documented its security program appropriately within the VRS IT Security Policy, VRS IT User Security Policy and the VRS Security Standard. Beneath the dictated requirements in the VRS Security Standard, VRS has created policies, procedures, guides and hardening documents to govern and direct related topic areas within each program's area. Additionally, we found VRS had contingency protections in place to hedge against risk of uncertain loss. Overall, we found the majority of these policies and procedures to be documented and updated appropriately. However, a handful of procedures and hardening guides were not reviewed and updated at least annually in accordance with the VRS Security Standard. Such observations are discussed further below and within the Recommendations section of the report.

BUSINESS CONTINUITY



VRS reengineered its Business Continuity plans in fiscal year 2020, resulting in a more detailed and comprehensive Enterprise Continuity Plan and supporting documents. The Enterprise Continuity Plan defines four Continuity Plan Teams, each with a distinct purpose and specific responsibilities. We found that for the audit period, VRS had adequate Business Continuity plans in place to reasonably ensure its ability to recover vital business operations in the case of a disaster.

VRS has created a comprehensive Enterprise Continuity Plan along with related plans including the IT Disaster Recovery Plan, Pandemic Response Plan, Facilities Recovery Plan and Department Recovery Plans to guide responsible personnel with the necessary recovery processes. These plans are supported by Business Impact Analysis, IT System and Data Sensitivity Classification and Risk Assessment documents. Specifically, VRS documented individual disaster recovery plans for sensitive systems and departments and developed test scenarios to switch from primary processing facilities to alternate processing facilities.

During our review, VRS was in the process of performing the annual self-assessment of the VRS Enterprise Continuity Plan and its foundational documents. Per the VRS Security Standard and the [VITA Risk Management Standard](#), VRS must perform annual reviews and conduct a full revision at least once every three years. The last full revision of this documentation occurred in 2020. VRS was in the process of finalizing the 2021 annual assessment at the time of our review in the first quarter of 2022. As a result, we were unable to evaluate an updated version reflecting an annual review for calendar year 2021. This observation is discussed further in the Recommendations section of the report.

While VRS did not conduct an official test of its Enterprise Continuity Plan in the calendar year 2020, the COVID pandemic provided VRS with a real-world scenario that identified opportunities to enhance and clarify the Enterprise Continuity Plan. VRS began operating in a continuity of operations state in March 2020. During the pandemic, VRS continued to perform all functions using primary processing facilities while VRS' human resources predominantly worked remotely.

SECURITY AWARENESS OPERATIONAL MEASURE

The **measure** calculates the percentage of **eligible staff** who have **completed** security training in **compliance** with the agency's and Commonwealth's security **policies**.

The calculation **methodology** of this OM states that "**Employees who join the agency during FY 2022 are required to complete SAFE training within 30 days after their start date. Staff who were hired prior to FY 2022 are required to complete the training once during FY 2022**".

However, VRS did not complete testing of all disaster recovery plans and test scenarios in 2020 and 2021. This observation is discussed further in the Recommendations section of the report.

Per VRS Security Standard section CP-3, VRS must train new business continuity personnel within 30 days of assuming a contingency role; when required by information system changes; and annually thereafter. VRS did not complete training for three new business continuity personnel within 30 days, and VRS did not complete training for members of all continuity plan teams in 2020 and 2021. This observation is discussed further in the Recommendations section of the report.

USER SECURITY AWARENESS

Security Awareness Training

We found VRS performs the required annual security awareness training. This annual training class is a mandatory requirement within AT-2 of the VRS Security Standard and [VITA's Cybersecurity Training Standard](#). We did not identify any VRS employees, including new hires or contractors, who had not completed the training course.

VRS training materials for the security awareness class exceeds the minimum training criteria requirements as listed in VRS Security Standard AT-2-COV and [VITA's Cybersecurity Training Standard](#). These materials included all required training to ensure each system user is aware of and understands applicable IT concepts, along with the user's acceptance of VRS security policies after completion of the security training.

As discussed in the Background, in addition to the minimum-security awareness standards promulgated by VITA, VRS routinely incorporates security awareness throughout the year into its "VRS Today" meetings, quarterly focused training modules, monthly phishing exercises, cyber security week activities, and screen saver and hall monitor messages.

Role-Based Training

VRS is required to provide role-based security training to personnel with assigned security roles and responsibilities before authorizing access to the system or performing assigned duties as dictated by AT-3 in the VRS Security Standard and [VITA's Cybersecurity Training Standard](#). Additionally, these requirements dictate that the Agency Head receives role-based training related to the position responsibilities and requirements of the Commonwealth's information

security program. We reviewed the training materials for these role-based trainings and found required training curriculum requirements were included and required personnel had completed their associated role-based training.

DATA PROTECTION

Overall, VRS has appropriately established data protection policies and procedures and communicated these regularly through VRS security awareness trainings to assist personnel with safeguarding VRS information and data, no matter the location of the authorized individual. VRS has deployed appropriate encryption mechanisms to protect all types of IT assets within its internal network, including the protection of transmission and authenticity of email and attached data that are considered sensitive relative to integrity and confidentiality. Additionally, VRS has implemented logging and monitoring practices to identify any evidence of unauthorized disclosure of organizational information.

However, certain opportunities to improve the processes surrounding VRS personnel international travel were identified and are discussed further in the Recommendations section of this report.

INFORMATION SYSTEM BACKUPS

With regard to system availability, VRS has adequate backup policies and procedures in place for applicable systems. VRS has backup plans in place to support restoration of systems, data and applications. Implemented procedures are documented and support safeguarded handling of all backup media with encryption mechanisms in place for data protection. Further, the procedures used to perform backups and the responsible parties who can send or request backups to be retrieved are segregated appropriately and aligned with the least privilege principle.

However, the procedures to perform and restore database backups were not fully documented. The documentation of the holistic process surrounding these were found to be reasonable, however the details surrounding the implementation of these processes were not memorialized appropriately to mitigate related risks or define and communicate the approved process for users approved by management. Specifically, VRS' process resulted in the creation of Service Level Agreements (SLA) between IT and the system owners of each database intended to define the foundation of the process and stipulate the agreed upon backup and restoration requirements and retention time periods. However, when reviewed, these SLAs were found to be incomplete and out of date.

SERVICE LEVEL AGREEMENTS AND VRS RETENTION

As noted in the **Follow-up on Previous Reports section**, management has initiated a project to review and update its **Retention and Disposition Schedules**.

Once this **framework** is completed, VRS should **reconcile** these **SLAs** with these newly developed **schedules** to ensure that **databases backups** are **aligned** with these newly established **timeframes**.

Once brought to management's attention, VRS immediately began work to improve backup and restoration process documentation. Management initiated the development of new procedural documentation which laid out detailed steps to support the approved backup and restoration process. As management finalizes this documentation, they should consider the implementation of regular exercises for testing sensitive system database backups to ensure they are functioning as expected and the data is present in a useable form as dictated in VRS Security Standard section CP-9-COV.

VRS also commenced improvements around the SLA process to ensure that these documents remained current, complete and aligned with organization objectives. To accomplish this, VRS began the process of developing SLA procedures which will guide these foundational documents and their regular review. VRS set the goal of having these procedures and all SLAs updated by December 31, 2022, with the institution of an annual review process thereafter to ensure that SLA timeframes are still adequate and timeframes continue to align with BIA Recovery Time Objectives.

We commend VRS for beginning the immediate development of this governance documentation to ensure that database backup and restoration processes can be performed completely and ensuring that backup timeframes continue to be aligned with overall agency goals.

CHANGE MANAGEMENT

Patch Management

VRS patching is performed appropriately through the change management process ensuring these patches are fully tested, reviewed and approved prior to patches being implemented in the production environment. Patching processes were in place to regularly patch VRS assets within 30 days of non-critical vulnerabilities being discovered, which exceeds the 90-day timeframe that the VRS Security Standard SI-2 requires. Further, evidence reviewed supported critical vulnerabilities being addressed immediately in accordance with VRS' procedures.

Data Fix Process

Overall, the data fix process is functioning as designed, however, we discussed with management certain opportunities to enhance existing segregation of duties, monitoring processes and controls to further mitigate the risk of undetected updates to records other than those defined

in the data fix request. Other observations regarding the data fix process are discussed further in the Recommendations section of this report.

ASSET MANAGEMENT

Asset and License Inventory

During the time of the examination, VRS was in the process of replacing the asset inventory tool prior to it reaching unsupported status in Spring 2022. As previously noted, we will review the new tool's processes during an upcoming future examination. The following observations were noted during the review of VRS' management of its assets including software licenses.

System Maintenance

The VRS Security Standard section MA-1 dictates that VRS develops and documents the organization's system maintenance policy and procedures. Presently, VRS has not created any system maintenance policies and procedures and instead relies on any language dictated in the maintenance clauses of the asset's contract. Management had previously recognized the need to address the creation or update of various procedures which are required within the VRS Security Standard including these and contracted with a vendor for support in this effort in 2021. Management expects to complete this extensive documentation project by the end of the calendar year 2022.

For onsite system maintenance performed by a contracted technician, access to equipment and building locations are controlled by the VRS Building Security Policy which requires VRS personnel to escort the technician at all times. As VRS had no system maintenance policy during the audit period defining organizational procedures when an asset is removed from VRS' control and taken offsite for maintenance, we inquired if any assets had been taken offsite then returned to VRS during 2021 and 2022 to assess the handling such equipment within VRS Security Standard's mandatory requirements. VRS confirmed that no assets had been removed from VRS for maintenance during this time period.

Portable Storage Devices

VRS management of portable storage devices was adequate and in compliance with mandatory requirements. We also confirmed these devices are not being used to transfer information from VRS sensitive systems.

Prohibited Services, Hardware and Software

We validated VRS' compliance and confirmed VRS has not contracted with or installed any prohibited software or hardware listed in [VITA's Prohibited Hardware, Software and Services Policy](#).

Asset Disposal

VRS sanitizes its assets prior to disposal or release from organizational control with the strength and integrity commensurate with the asset's security classification as required in the VRS Security Standard MP-6. VRS disposal processes for media was adequate and ensured VRS data is protected prior to release.

Use of Unsupported Systems

We found the status of all systems was being monitored and the majority of VRS systems were currently supported. Further, VRS has multiple projects underway to replace equipment prior to equipment reaching unsupported status. However, two devices active in the VRS environment had already reached an unsupported status. Both these devices were planned to be replaced and removed from the status prior to the end of this examination, however due to a design change and COVID supply chain delays these projects were not completed as of the issue date of this report.

We discussed with management additional mitigating actions or controls implemented by VRS during the unsupported time of these devices to ensure known risks are mitigated while they remain active in VRS' IT environment. We found management's planned actions surrounding the mitigation of the possible impact of these devices in vulnerable status to be reasonable and noted VRS will continue the close monitoring of these devices until they are removed from the network and plans to file the appropriate VITA compliance exception extensions, as necessary. We support management's ongoing efforts to replace all devices prior to reaching an unsupported status to mitigate the resulting risks of unsupported systems.

Of additional note, VRS' existing asset management system was close to reaching a vulnerable status, however, during the course of this engagement it was replaced by VRS prior to reaching unsupported status. Full implementation of the new system will allow VRS to centralize its monitoring process, streamline its ability to confirm completeness of the VRS IT asset population,

identify unsupported dates more effectively and assist VRS' ability in replacing systems prior to reaching unsupported dates.

THREAT MANAGEMENT

VRS has appropriately implemented various products and third-party services to reasonably detect, log, report and manage potential or real attacks or threats to the VRS IT infrastructure. This implementation includes configuration of protective systems which overlap each other to some degree to provide a level of redundant coverage in the event a protective system fails or responds ineffectively. Further, we found VRS to be providing summary reports timely to VITA Commonwealth Security as dictated in the VRS Security Standard IR-6-COV and IR-6-COV-VRS.

Incident Response Plan

At the time of our review, VRS was in the process of updating its IRP. Even in draft form, VRS has a formal documented IRP plan which lays out a framework and set of processes to be followed during the occurrence of a security incident. The VRS IRP is adequate and in compliance with the *Code of Virginia* in regard to mandatory breach notification to affected parties. Since the IRP was in flux, we offered suggested improvements based on our review of the draft document.

Additionally, VRS has a plan in place to work with the Virginia Attorney General on proper notification should a breach occur at VRS for a retiree or beneficiary who resides in another state or country.

Finally, we found that there were no incidents during 2021 which elevated to the level which activated the IRP nor could we identify any scenarios in which the IRP should have been activated. While a positive result for VRS, we can draw no conclusions regarding VRS' compliance with its IRP or resulting documentation of any specific events.

Vulnerability Assessments and Penetration Testing

During 2021, VRS consistently performed vulnerability assessments at least quarterly and penetration tests annually or more frequently if required to address an environmental change on VRS systems. After testing, VRS remediated and retested findings that were noted to ensure that VRS adequately corrected vulnerabilities.

Externally Managed Facilities

We found VRS had documented their review of SSAE 18 report to ensure VRS assets are protected appropriately from any third-party risks. Further, we found physical access was managed appropriately through the facilities' access system.

However, evidence of VRS' consideration or management of expected complementary user entity controls identified in the SSAE 18 report was unavailable for the audit period. The management of these controls were addressed in an outstanding recommendation from the Vendor Hosted Systems in Administrative Operations ([Report No. 439](#)) called "Enhance Risk Monitoring of Hosted System Vendors". In response to this recommendation, VRS plans to implement a new tool and will capture these requirements under each particular vendor to track the control's implementation. We will perform a limited review of this updated process once management represents this recommendation as implemented.

Lastly, we determined VRS had appropriately requested and received approval from VITA for an exception to VRS Security Standard section PE-1-COV. While VRS' IT environment currently requires this exception, management is actively working to address the cause.

FOLLOW-UP ON PRIOR REPORTS

Per review of the Audit Recommendation Follow-up System (ARFUS), two audit recommendations remain outstanding from our previous audit ([Report No. 425](#)). The status of these recommendations are as follows:

- The recommendation titled "Enhance Management of Policy and Procedure Documents" was represented as completed as of January 31, 2022 and will be reviewed in our upcoming FY22 Annual ARFUS review.
- The recommendation titled "Update Retention and Disposition Schedules to align with Library of Virginia Standards as well as VRS Actual Practice" remains outstanding. Currently, the planned completion date for the outstanding recommendation has not been set by management at this time. However, management has placed focus on their response to this recommendation by highlighting it as one of four key agency performance objectives for fiscal year 2022. We will continue to monitor this finding through the ARFUS process.

REPORTABLE CONDITION

Any observation included in the Recommendations section of the report is considered a “Reportable Condition.” The resolution of a “Reportable Condition” merits monitoring in the Audit Recommendation Follow-Up System (ARFUS).

MATERIAL ISSUE

Certain recommendations may address a matter that poses such significant risk to VRS whereby immediate measures should be taken to mitigate the exposure. Other long-term solutions may also be appropriate for the permanent resolution of the matter. These recommendations are considered a “Material Issue.”

All recommendations require a formal response from management.

Due to their unimplemented status at the commencement of this review, we exempted these areas from the scope of this review.

RECOMMENDATIONS

We offer the following recommendations as a result of this examination, none of which are considered a “Material Issue.”

1. Ensure Completion of Required Continuity Plan Testing, Training Exercises and Review

The effective development, maintenance and implementation of an organization’s Enterprise Continuity Plan requires a multi-layered effort of ongoing reviews, testing, and training. Opportunities to ensure the plan meets the needs of the organization, is achievable as designed and understood by all responsible parties were observed during the course of this review.

IT Disaster Recovery Testing

The VRS Security Standard sections CP-1-COV-2 & CP-4 require annual testing of the IT disaster recovery plan. While COVID offered the opportunity to validate in real time components of the Enterprise Continuity Plan, VRS did not complete testing of the IT disaster recovery plan and test scenarios in 2020 or 2021. A similar observation was made during the previous examination of this area ([No. 425](#)). Management should conduct annual testing to determine the effectiveness of the IT disaster recovery plan and to assess the organizational readiness to execute the IT disaster recovery plan and respond to a disaster.

Enterprise Continuity Plan Training

The VRS Security Standard section CP-3 states that VRS must train new business continuity personnel within 30 days of assuming a contingency role; when required by information system changes; and annually thereafter. VRS did not complete training for new business continuity personnel within 30 days of assuming a contingency role or responsibility, and VRS did not complete training for members of all continuity plan teams in 2020 and 2021. This is a repeat area of discussion which has been identified during in our previous two examinations of this area (Report [No. 367](#) & [No. 425](#)). Management should ensure that all business continuity personnel receive training on their roles and responsibilities within 30 days of assuming a contingency role

or responsibility and annually thereafter as well as receiving training when required as a result of information system changes.

Enterprise Continuity Plan Review

Per the VRS Security Standard, VRS must review and update contingency planning policy and procedures on an annual basis or more frequently if required to address an environmental change. The VRS Security Standard also elaborates that a full revision of the Business Impact Analysis and the Risk Assessment documents, foundational to the VRS Enterprise Continuity Plan, must be performed at least once every three years with annual self-assessments during the years in between. While a comprehensive update was completed in 2020, as of the end of the first quarter of 2022, the 2021 annual review of the Business Impact Analysis, Risk Assessment and Enterprise Business Continuity Plan and related documents was still underway. Management should ensure the timely completion of annual reviews to assess the continued validity of the information and to determine if any changes are required.

An underlying theme which may have impacted VRS' execution of each of these items is the availability of sufficient staffing resources to achieve them. VRS recognized the need to supplement its existing resources through the use of consulting services when it performed its most recent update to the Enterprise Continuity Plan and those efforts resulted in the most comprehensive plan to date. Significant investments into VRS' IT Resources have been made over the past several years and continued enhancements were approved by the Board for the upcoming biennial budget. Once approved by the General Assembly, the successful implementation of these planned initiatives and staffing enhancements should aid in VRS' efforts to address these opportunities. However, the speed of the implementation may be hampered by current challenges with recruitment being universally experienced as a result of the limited pool of qualified IT resources.

2. Improve Configuration and Procedural Documentation Update Process

Technology is constantly evolving which requires VRS to continuously adapt to its ever-changing environment. VRS has developed and implemented many documents outlining VRS procedures, hardening configurations and guides relative to VRS business process. We commend management for their efforts as these procedures and guides help to ensure knowledge transfer between VRS personnel and assist in the assurance that only approved procedures and settings are implemented.

During this review, we noted various governance and configuration documentation had not been reviewed and updated regularly or within the last year. In some cases, updates had not occurred for several years. Further, the VRS Security Standard section CM-2 requires sensitive systems hardening configuration documentation to be updated on an annual basis or more frequently if requested to address an environmental change.

Along with planned enhancements to VRS' operating environment, the COVID pandemic created a new normal, revised organizational and resource priorities and led to adjustments in the IT environment which impacted the previous triggers used to initiate the regular review of IT governance documents. Specifically, pre-pandemic, VRS had developed an application for maintaining IT security program documentation which tracked and managed the regular update process. Each document in the application was owned by specific staff member who was automatically notified through email when routine reviews for update were necessary. The application stopped functioning properly and did not provide the expected notifications, leading to delays, sometimes significant, in the timing of governance document reviews.

VRS recently initiated several projects which should ultimately support the future management of its governance documents. VRS should continue its efforts to implement a new mechanism or modify the existing application to ensure ongoing monitoring of governance documentation and timely prompting for documentation review and update by responsible parties. These reviews and updates should include a formal approval process for substantive changes to the documentation to ensure adjusted procedures implement authorized settings to secure the VRS environment appropriately and continue VRS' compliance with mandatory requirements.

3. Fortify Processes Surrounding Devices Used for International Travel

VRS must implement additional security controls to mitigate risks when an individual uses a VRS owned device outside of the country. These configurations are in place for individuals permanently working internationally. However, VRS must work with VRS personnel who temporarily travel internationally to ensure they have appropriately configured devices prior to such travel. VRS communicates the need for VRS personnel to report planned international travel prior to traveling through annual security trainings and the IT department's mobility support page.

PERSONAL DEVICE PROGRAM

The VRS PDP allows employees to use their own mobile devices for business purposes. This initiative allows staff to access VRS systems and data while ensuring that VRS systems and data are protected from unauthorized access, use or disclosure.

However, VRS does not have approved documented procedures, based on the requirements set forth in the VRS Security Standard CM-2-COV (4) to direct IT staff how to consistently configure VRS devices used during international travel. To ensure VRS IT staff are appropriately configuring VRS owned devices before and after international travel, VRS should memorialize approved configuration standards and the procedures to apply them.

Further, VRS' policies do not address the configuration of personal devices used through the Personal Device Program (PDP) during international travel by VRS personnel. We inquired but were unable to confirm that the existing security configurations forced to PDP enrolled devices would be sufficient to meet security requirements necessary to protect VRS' data during international travel. VRS should investigate and determine if available PDP device security configurations meet international travel requirements. If appropriate international security configurations cannot be met for these devices (as VRS cannot control certain security aspects on these devices because they are personally owned), VRS should disable access to PDP applications for the enrolled device until the individual returns from their international travel, similarly to device functions which would be disabled on a VRS laptop for the same reason.

As we discussed this observation with management, VRS communicated they plan to create an International Travel Policy during the calendar year 2022 which will include the development of corresponding procedure documents with specified requirements to support the execution of the policy over both VRS owned and PDP devices. We encourage VRS to proceed with this plan while ensuring the configuration needs for VRS and personally owned devices are addressed when on business or personal international travel.

Further, when disseminating security training or topics, VRS has historically gone above and beyond by providing VRS personnel security tips to apply at home or outside the workplace. Since VRS does not have full control over PDP devices, management should further educate members on recommended security measures on these devices to supplement the individual's and agency's data protection. When discussed with management, they were supportive and indicated they would investigate including additional guidance in the upcoming annual training.

4. Enhance Data Fix Processes and Controls

VRS uses the data fix process to adjust and correct records within VNAV that cannot be made through the application. These adjustments and corrections can be for a single record or for multiple records and may be a one-time update or become a recurring update, depending on the business need and their complexity. Because of the reliance VRS places on the data fix process to maintain data quality in VNAV, various controls exist to ensure only intended records are updated and data fixes fully address all data elements requiring update.

During our review, no instances of unauthorized updates were identified, however, several observations during the course of the examination revealed opportunities to enhance the existing data fix process and provide additional assurance over the completeness of data fixes. The opportunities include:

- Implementing additional techniques to ensure all related data touchpoints are considered when data is identified for update;
- Establishing a process to periodically review and update, as needed, the list of tables subject to audit as part of the monitoring changes made through the data fix process along with defining the ownership of the responsibility for making the determination of which tables should be audited; and,
- Enhancing existing policies and procedures to reflect current practices as well as documentation of unit testing results and end user validation activities.

Implementing some or all of these process enhancements in conjunction with VRS' existing compensating controls will further mitigate the inherent risks present in this type of system maintenance (data adjustments and corrections) and potentially minimize the need for later rework.

MANAGEMENT EXIT CONFERENCE

This report was distributed to Ms. Bishop and other members of VRS' management and staff for review and comment. They expressed substantial agreement with this report and will issue a written response to the recommendations contained in this report.

REPORT DISTRIBUTION

Submitted to the Audit and Compliance Committee at its meeting held
June 16, 2022.

MEMBERS OF THE AUDIT AND COMPLIANCE COMMITTEE

Joseph W. Montgomery, Committee Chair, Board Vice Chair
W. Brett Hayes, Committee Vice Chair
A. Scott Andrews, Board Chair

WITH COPIES TO:

OTHER MEMBERS OF THE BOARD OF TRUSTEES

J. Brandon Bell, II
John M. Bennett
Michael P. Disharoon
William A. Garrett
Susan T. Gooden
Troilen G. Seward

VRS EXECUTIVE LEADERSHIP

Patricia S. Bishop
Ronald D. Schmitz
Members of the Director's
Executive Committee

AUDITOR OF PUBLIC ACCOUNTS

Staci Henshaw

JLARC

Kimberly A. Sarte
Jamie Bitz

PRINCIPAL AUDITOR IN-CHARGE

Matthew Priestas, CIA, CRMA, CISA, PMP

PRINCIPAL AUDITOR – DATA ANALYTICS

Krystal Groff, CIA, CISA

AUDIT SUPERVISOR

Judy Bolt, CPA, CIA, CISA, CFE



To: Jennifer P. Bell Schreck, Internal Audit Director

From: Patricia S. Bishop, Director *PSB*

Date: June 10, 2022

Subject: Management's Response to Internal Audit Report No. 444 – "Review of IT General Controls"

We reviewed the above captioned Internal Audit Report on "Review of IT General Controls". We appreciate the Internal Auditor's analysis and comments regarding the emphasis VRS places on technology security and the effectiveness of its overall application control environment. We also appreciate the thorough background provided in the report as well as the professionalism and cooperation exhibited by internal audit staff.

Beginning in March 2020, VRS, like many organizations, implemented fulltime remote work for most of its employees as a result of the COVID 19 pandemic. Due to the agency's emergency preparedness and technological enhancements, staff was able to transition to remote work seamlessly, with no disruption in services to its members. Further, the pandemic provided an opportunity for VRS Information Technology team to evaluate its systems and plan for additional improvements to support continued remote work in the future.

While the world seemed to slow down during the pandemic, information security threats continued to persist, and that remains true today. Combined with supply chain disruptions and changes in the human capital market, the information security industry has been severely challenged over the last two years. This has impacted the VRS Information Security team as well. Nevertheless, the team remains steadfastly focused on protecting the agency's data, ensuring that clear and present dangers to the organization are given priority over other assignments. In addition, the team has committed significant resources to ongoing training for staff, including virtual learning programs, phishing exercises, cybersecurity awareness events and monthly updates to staff through the agency's VRS Today webinars.

Given the constraints noted above, the team is working on additional information security elements, including policy and procedure updates, and continuity of operations plan testing. The team recognizes the importance of ensuring that these components of the overall program

are current and has developed a plan to accomplish them, as outlined in the responses below. While working to accomplish these tasks by the target dates provided, the VRS Information Security Team's main priority will remain the day-to-day security of the agency's data and ensuring that all members of staff understand their role in information security.

Management looks forward to continuing its partnership with Internal Audit, identifying and addressing challenges to information security on an ongoing basis, beyond the regular audit cycle, to ensure the compliance of our technology systems.

The Audit Report identified four recommendations that require follow-up. Below is the recommendation and management's response.

1. Ensure completion of required continuity plan testing, training exercises and review.

The effective development, maintenance and implementation of an organization's Enterprise Continuity Plan requires a multi-layered effort of ongoing reviews, testing, and training. Opportunities to ensure the plan meets the needs of the organization, is achievable as designed and understood by all responsible parties were observed during the course of this review.

IT Disaster Recovery Testing

The VRS Security Standard sections CP-1-COV-2 & CP-4 require annual testing of the IT disaster recovery plan. While COVID offered the opportunity to validate in real time certain components of the Enterprise Continuity Plan, VRS did not complete testing of the IT disaster recovery plan and test scenarios in 2020 or 2021. A similar observation was made during the previous examination of this area (No. 425). Management should conduct annual testing to determine the effectiveness of the IT disaster recovery plan and to assess the organizational readiness to execute the IT disaster recovery plan and respond to a disaster.

Enterprise Continuity Plan Training

The VRS Security Standard section CP-3 states that VRS must train new business continuity personnel within 30 days of assuming a contingency role; when required by information system changes; and annually thereafter. VRS did not complete training for new business continuity personnel within 30 days of assuming a contingency role or responsibility, and VRS did not complete training for members of all continuity plan teams in 2020 and 2021. This is a repeat area of discussion which has been identified during in our previous two examinations of this area (Report No. 367 & No. 425). Management should ensure that all business continuity personnel receive training on their roles and responsibilities within 30 days of assuming a contingency role or responsibility and annually thereafter as well as receiving training when required as a result of information system changes.

Enterprise Continuity Plan Review

Per the VRS Security Standard, VRS must review and update contingency planning policy and procedures on an annual basis or more frequently if required to address an environmental

change. The VRS Security Standard also elaborates that a full revision of the Business Impact Analysis and the Risk Assessment documents, foundational to the VRS Enterprise Continuity Plan, must be performed at least once every three years with annual self-assessments during the years in between. While a comprehensive update was completed in 2020, as of the end of the first quarter of 2022, the 2021 annual review of the Business Impact Analysis, Risk Assessment and Enterprise Business Continuity Plan and related documents was still underway. Management should ensure the timely completion of annual reviews to assess the continued validity of the information and to determine if any changes are required.

An underlying theme which may have impacted VRS' execution of each of these items is the availability of sufficient resources to achieve them. VRS has strong history of sound financial management and has always worked to provide the most to benefit its members while minimizing the cost to do so. VRS recognized the need to supplement its existing resources when it performed its most recent update to the Enterprise Continuity Plan and those efforts resulted in the most comprehensive plan to date. Significant investments into VRS' IT Resources have been made over the past several years and were approved by the Board for the upcoming biennial budget. Once approved by the General Assembly, the planned initiatives and enhancements to VRS' IT Resources should aid in its efforts to address these opportunities.

Management's Response: *As noted in the report, the Security Operations department has experienced turnover and as a result has been working with limited resources. In addition, hiring highly skilled, experienced and talented personnel has been a challenge. The Information Technology team is currently working with Human Resources and an external recruiter to identify and hire full-time VRS staff members. Concurrently, leadership is interviewing consulting companies to assist with short- and long-term staff augmentation.*

IT Disaster Recovery Testing

VRS is supporting a primarily remote work force which offered the opportunity to validate certain components of the Enterprise Continuity Plan and the IT Disaster Recovery Plan. VRS plans to conduct a tabletop IT disaster recovery test, which is expected to be completed by December 31, 2022. VRS also plans to perform another test once migration to the new datacenter concludes in 2023.

Enterprise Continuity Plan Training

VRS will be reviewing and revising the workflow in RAMS around the business continuity roles. The improvement to RAMS will include a new notification for mandatory training of personnel whose roles include continuity of operations. RAMS changes are expected to be completed by August 1, 2022.

VRS will complete annual training of all continuity team members by August 1, 2022.

Enterprise Continuity Plan Review

While the final edits on the 2021 BIA and Risk Assessment updates have not been completed, the data gathering to perform those updates was completed in 2021. Those updates are foundational to completing the overall updates to the Enterprise Continuity Plan. This work is expected to be completed by August 1, 2022, across all VRS business units.

2. Improve configuration and procedural documentation update process.

Technology is constantly evolving which requires VRS to continuously adapt to its ever-changing environment. VRS has developed and implemented many documents outlining VRS procedures, hardening configurations and guides relative to VRS business process. We commend management for their efforts as these procedures and guides help to ensure knowledge transfer between VRS personnel and assist in the assurance that only approved procedures and settings are implemented.

During this review, we noted various governance and configuration documentation had not been reviewed and updated regularly or within the last year. In some cases, updates had not occurred for several years. Further, the VRS Security Standard section CM-2 requires sensitive systems hardening configuration documentation to be updated on an annual basis or more frequently if requested to address an environmental change.

Along with planned enhancements to VRS' operating environment, the COVID pandemic created a new normal, revised organizational and resource priorities and led to adjustments in the IT environment which impacted the previous triggers used to initiate the regular review of IT governance documents. Specifically, pre-pandemic, VRS had developed an application for maintaining IT security program documentation which tracked and managed the regular update process. Each document in the application was owned by specific staff member who was automatically notified through email when routine reviews for update were necessary. The application stopped functioning properly and did not provide the expected notifications, leading to delays, sometimes significant, in the timing of governance document reviews.

VRS recently initiated several projects which should ultimately support the future management of its governance documents. VRS should continue its efforts to implement a new mechanism or modify the existing application to ensure ongoing monitoring of governance documentation and timely prompting for documentation review and update by responsible parties. These reviews and updates should include a formal approval process for substantive changes to the documentation to ensure adjusted procedures implement authorized settings to secure the VRS environment appropriately and continue VRS' compliance with mandatory requirements.

Management's Response: *The SharePoint repository is being migrated to SharePoint Online, which is a component of Microsoft 365 (M365). A new workflow will be implemented in the new SharePoint Online site to manage the document update process. The implementation of the revised SharePoint workflow will be completed by April 1, 2023.*

3. Fortify processes surrounding devices used for international travel.

VRS must implement additional security controls to mitigate risks when an individual uses a VRS owned device outside of the country. These configurations are in place for individuals permanently working internationally. However, VRS must work with VRS personnel who temporarily travel internationally to ensure they have appropriately configured devices prior to such travel. VRS communicates the need for VRS personnel to report planned international travel prior to traveling through annual security trainings and the IT department's mobility support page.

However, VRS does not have approved documented procedures, based on the requirements set forth in the VRS Security Standard CM-2-COV (4) to direct IT staff how to consistently configure VRS devices used during international travel. To ensure VRS IT staff are appropriately configuring VRS owned devices before and after international travel, VRS should memorialize approved configuration standards and the procedures to apply them.

Further, VRS' policies do not address the configuration of personal devices used through the Personal Device Program (PDP) during international travel by VRS personnel. We inquired but were unable to confirm that the existing security configurations forced to PDP enrolled devices would be sufficient to meet security requirements necessary to protect VRS' data during international travel. VRS should investigate and determine if available PDP device security configurations meet international travel requirements. If appropriate international security configurations cannot be met for these devices (as VRS cannot control certain security aspects on these devices because they are personally owned), VRS should disable access to PDP applications for the enrolled device until the individual returns from their international travel, similarly to device functions which would be disabled on a VRS laptop for the same reason.

As we discussed this observation with management, VRS communicated they plan to create an International Travel Policy during the calendar year 2022 which will include the development of corresponding procedure documents with specified requirements to support the execution of the policy over both VRS owned and PDP devices. We encourage VRS to proceed with this plan while ensuring the configuration needs for VRS and personally owned devices are addressed.

Further, when disseminating security training or topics, VRS has historically gone above and beyond by providing VRS personnel security tips to apply at home or outside the workplace. Since VRS does not have full control over PDP devices, management should further educate members on recommended security measures on these devices to supplement the individual's and agency's data protection. When discussed with management, they were supportive and indicated they would investigate including additional guidance in the upcoming annual training.

Management's Response: *The VRS Service Desk has an existing process to support travel outside the United States. When an employee is planning to travel outside of the United States, they will contact the VRS Service Desk who provides VRS resources that are required while traveling. For example, a loaner laptop may be made available during travel and then wiped when it returns. Additional communication to staff via various channels will be provided regarding the steps that need to be taken if traveling internationally and requiring access to VRS resources.*

VRS recognizes a need to document, update and strengthen our mobile device travel policies. Staff will conduct a holistic review of the mobile device and Bring Your Own Device (BYOD) program to include VRS and personal devices, Azure tenant and Intune configurations, policies and standards. This work is expected to be completed by June 30, 2023. An international travel policy is currently in draft form and is expected to be published prior to October 31, 2022.

4. Strengthen Data Fix Processes and Controls

VRS uses the data fix process to adjust and correct records within VNAV that cannot be made through the application. These adjustments and corrections can be for a single record or for multiple records and may be a one-time update or become a recurring update, depending on the business need and their complexity. Between January 1, 2021, and September 30, 2021, VRS staff entered 2,149 data fix requests which were not cancelled. Because of the reliance VRS places on the data fix process to maintain data quality in VNAV, it is critical controls exist to ensure only intended records are updated and data fixes fully address all data elements requiring update.

Current process and controls provide a limited level of assurance over the completeness of the data fix process. Several observations during the course of the examination revealed opportunities to strengthen the data fix process and the controls. The opportunities include:

- Formally documenting policies and procedures as well as unit testing results and end user validation activities;
- Implementing additional techniques to ensure all related data touchpoints are considered when data is identified for updated; and,
- Establishing a process to periodically review and update, as needed, the list of tables subject to audit as part of the monitoring changes made through the data fix process along with defining the ownership of the responsibility for making the determination of which tables should be audited.

During our review, no instances of unauthorized updates were identified, however the strengthening of the controls surrounding some or all of these processes will further mitigate risks which inherently relate to this type of system maintenance (data adjustments and corrections) and potentially minimize the need for later rework.

Management's Response: Management has shared its controls with Internal Audit and will establish a process to review new data tables and consider their potential for data fix monitoring. This analysis is expected to be completed by June 30, 2023. Further, VRS may verify and enhance, as needed, the current and established documentation.

Miscellaneous Updates

Report of Alleged Fraud, Waste and Abuse Hotline Cases

**For Complaints Received During the Period
February 1, 2022 through April 30, 2022**

SUMMARY OF CASES REVIEWED AND CLOSED

During the period February 1, 2022, through April 30, 2022, we received no cases of potential Fraud, Waste and Abuse from the Office of the State Inspector General.

Background

Fraud, Waste and Abuse relating to VRS can be comprised of any number of concerns. Such items can be reported to VRS' Internal Audit Department directly or through the Office of the State Inspector General (OSIG) State Employee Fraud, Waste and Abuse Hotline. (A majority of complaints are received through OSIG.)

All matters that relate to Fraud, Waste and/or Abuse reported are reviewed to determine the proper protocol for investigation.

Committee Reporting

Cases of a serious and/or significant nature will be reported to the VRS Audit and Compliance Committee immediately. At a minimum, a summary of all Hotline cases will be reported to the Audit and Compliance Committee on a quarterly basis.

Retention

Hardcopy documents, including handwritten notes, are stored in a secure location until the case is closed, upon which they are shredded. Electronic files are stored on Internal Audit's secured drive. Documentation containing case details are labeled "**CONFIDENTIAL – STATE FRAUD, WASTE AND ABUSE HOTLINE DOCUMENTS**" and sensitive items are labeled FOIA Exempt. As appropriate, files are disposed of in accordance with the Library of Virginia's retention policy.

FRAUD, WASTE AND ABUSE CASE MANAGEMENT

PROCESSING OF COMPLAINTS

When received, the Audit Director and Hotline Auditor perform a preliminary review of the complaint. After initial discussion, the Hotline Auditor determines whether a formal response is required by OSIG (cases referred by OSIG may or may not require a formal response, depending on the nature of the complaint) and adds the case to Internal Audit's Hotline Tracking System.

The Hotline Auditor sets up a case file on Internal Audit's secured and restricted drive to maintain confidentiality. The Hotline Auditor then evaluates the case details and may review information available in VRS' systems to obtain further details about the subject of the complaint. Additionally, the Hotline Auditor may forward the details of the case to other VRS personnel for review. The Hotline Auditor also notifies the VRS Director of the case.

Complaints regarding disability benefits constitute the large majority of the Hotline cases received by VRS. The Hotline Auditor will meet with appropriate VRS staff, as necessary, to discuss details of the case in order for all parties to proceed forward with their portion of the investigation. Complaints forwarded to others are monitored for resolution. Actions and determinations for cases are reviewed for reasonableness by the Hotline Auditor. Once a determination of appropriate action has occurred, such action is documented in the Internal Audit case file and on the Hotline Tracking System. The Internal Audit Director is apprised of all actions and determinations.

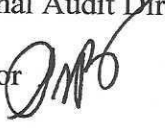
For other complaints, such as internal fraud, waste or abuse (examples could include abuses of various types of leave, teleworking policies, employee theft, etc.), the Hotline Auditor investigates the allegation and obtains supporting documentation from management, as needed. If a determination is made that there is a reasonable possibility of fraud, waste or abuse, management is notified of the allegation by the Audit Director and given a reasonable timeframe in which to report back to the Audit Director any actions taken regarding the allegation. The Audit Director determines the reasonableness of such action, reports the actions and resolution of the complaint to the Hotline Auditor who documents the results in the case file and on the Hotline Tracking System.

All investigation results are reported to the VRS Director and members of the VRS Audit and Compliance Committee once a case is resolved, regardless of the outcome.



Patricia S. Bishop
Director

MEMORANDUM

To: Jennifer P. Schreck, Internal Audit Director
From: Patricia S. Bishop, Director 
Date: June 3, 2022
Subject: Summary of Travel Related Expenses

I am attaching the following:

1. Summary of Travel Related Expenses Paid During the Quarter of and Fiscal Year-to-Date Through March 31, 2022.
2. Summary of Other Sponsored Travel Related Expenses Paid During the Quarter of and Fiscal Year-to-Date Through March 31, 2022. *There was no reportable Other Sponsored Travel Related Expenses for the period.*
3. Detail of Travel Related Expenses Paid During the Quarter of and Fiscal Year-to-Date Through March 31, 2022.
4. Record of Attendance and Per Diems for the Quarter Ended March 31, 2022.

This information should be shared with the Audit & Compliance Committee.

If you have any questions, please do not hesitate to ask.

PSB/lbk

Attachments

Summary of Travel Related Expenses
 Virginia Retirement System
 Board/Committee Members and Selected VRS Staff

Fiscal Year-To-Date **Q3 2022**

Traveler	Current Quarter Expenses											Fiscal Year-To-Date Expenses					
	Total Travel			Out-of-State-Travel								Total Travel			Out-of-State-Travel		
	Sponsor Paid	VRS Paid	Total	# Trips	Cost	Travel reasons							Sponsor Paid	VRS Paid	Total	# Trips	Cost
AM						BD	CF	DD	MM	SV	TR						
Beasley, Michael	-	-	-	-	-	-	-	-	-	-	-	-	-	\$2,948.36	\$2,948.36	-	-
Bell II, John	-	\$448.84	\$448.84	-	-	-	-	-	-	-	-	-	-	\$2,147.72	\$2,147.72	-	-
Disharoon, Michael	-	\$428.16	\$428.16	-	-	-	-	-	-	-	-	-	-	\$1,548.43	\$1,548.43	-	-
Economou, Theodore	-	774.76	\$774.76	-	-	-	-	-	-	-	-	-	-	\$774.76	\$774.76	-	-
Garrett, William	-	\$224.64	\$224.64	-	-	-	-	-	-	-	-	-	-	\$1,403.97	\$1,403.97	-	-
Lewis, Wilbert	-	-	-	-	-	-	-	-	-	-	-	-	-	\$1,109.86	\$1,109.86	-	-
McWilliams III, O'Kelly	-	\$580.55	\$580.55	-	-	-	-	-	-	-	-	-	-	\$3,365.21	\$3,365.21	-	-
Montgomery, Joseph	-	\$196.56	\$196.56	-	-	-	-	-	-	-	-	-	-	\$833.84	\$833.84	-	-
Seward, Troilen	-	\$157.95	\$157.95	-	-	-	-	-	-	-	-	-	-	\$672.03	\$672.03	-	-
Bishop, Patricia	-	\$1,128.72	\$1,128.72	-	-	-	-	-	-	-	-	\$935.31	\$1,336.79	\$2,272.10	1	\$1,143.38	
Schmitz, Ronald	-	\$367.88	\$367.88	-	-	-	-	-	-	-	-	-	-	\$367.88	\$367.88	-	-
Alouf, John	-	\$865.20	\$865.20	1	\$865.20	-	-	-	1	-	-	\$2,845.86	\$1,874.76	\$4,720.62	4	\$4,720.62	
Chang, Warren	-	-	-	-	-	-	-	-	-	-	-	\$2,102.00	\$1,118.59	\$3,220.59	3	\$3,220.59	
Coleman, Thomas	-	\$1,084.78	\$1,084.78	1	\$1,084.78	-	-	-	1	-	-	-	\$4,084.24	\$4,084.24	4	\$4,084.24	
Gentry III, William	-	\$1,547.94	\$1,547.94	1	\$1,547.94	-	-	-	-	1	-	-	\$1,547.94	\$1,547.94	1	\$1,547.94	
Jones, De'Von	-	-	-	-	-	-	-	-	-	-	-	-	\$2,195.78	\$2,195.78	2	\$2,195.78	
Matoua, Katherine	-	\$2,759.81	\$2,759.81	-	-	-	-	-	-	-	-	-	\$2,759.81	\$2,759.81	-	-	
Mulvin, Thomas	-	-	-	-	-	-	-	-	-	-	-	-	\$157.92	\$157.92	1	\$157.92	
Murphy, James	-	\$539.99	\$539.99	1	\$539.99	-	-	-	1	-	-	-	\$539.99	\$539.99	1	\$539.99	
Noland, Walker	-	-	-	-	-	-	-	-	-	-	-	-	\$266.08	\$266.08	1	\$266.08	
Sarki-Hurd, Hajara	-	-	-	-	-	-	-	-	-	-	-	-	\$3,046.84	\$3,046.84	1	\$220.64	
Total	-	\$11,105.78	\$11,105.78	4	\$4,037.91	-	-	-	3	1	-	\$5,883.17	\$34,100.80	\$39,983.97	19	\$18,097.18	

Travel Reasons Legend			
AM	Advisory/Assoc. Meeting	MM	Manager Meeting
CF	Conference	SV	Site Visit
DD	Due Diligence	TR	Training
BD	Board/Committee Meeting		

Detail of Travel Related Expenses
Virginia Retirement System
Board/Committee Members and Selected VRS Staff
Paid in Q3 2022

Traveler	Travel Start	Travel End	Destination	Sponsor	Purpose	Sponsor Paid	VRS Paid	Total
Bell II, John	12/02/2021	12/02/2021	Richmond, VA		Attended the Defined Contribution Plans Advisory Committee meeting.	-	\$219.52	\$219.52
Bell II, John	02/10/2022	02/10/2022	Richmond, VA		Attended Board of Trustees meeting.	-	\$229.32	\$229.32
Disharoon, Michael	02/09/2022	02/10/2022	Richmond, VA		Attended the Benefits and Actuarial Committee and Board of Trustees meetings.	-	\$428.16	\$428.16
Economou, Theodore	11/09/2021	11/10/2021	Richmond, VA		Travel from Switzerland to attend IAC meeting	-	\$774.76	\$774.76
Garrett, William	02/09/2022	02/10/2022	Richmond, VA		Attended the Benefits and Actuarial Committee and Board of Trustees meetings.	-	\$224.64	\$224.64
McWilliams III, O'Kelly	02/08/2022	02/10/2022	Richmond, VA		Attended the Administration and Personnel Committee, Benefits and Actuarial Committee and Board of Trustees meetings.	-	\$457.70	\$457.70
McWilliams III, O'Kelly	03/24/2022	03/24/2022	Richmond, VA		Attended the VRS Defined Contribution Plans Advisory Committee meeting.	-	\$122.85	\$122.85
Montgomery, Joseph	02/08/2022	02/10/2022	Richmond, VA		Attended the Administration and Personnel Committee, the Benefits and Actuarial Committee and Board of Trustees meetings.	-	\$196.56	\$196.56
Seward, Troilen	02/08/2022	02/10/2022	Richmond, VA		Attended the Administration and Personnel Committee, the Benefits and Actuarial Committee and the Board of Trustees meetings.	-	\$157.95	\$157.95
Bishop, Patricia	01/10/2022	01/10/2022	Richmond, VA		Presented at the VA Association of School Superintendents and VA Association of School Business Officials annual Winter Conference.	-	\$20.00	\$20.00
Bishop, Patricia	02/27/2022	02/28/2022	Washington, DC		Attended the National Association of State Retirement Administrators winter meeting.	-	\$1,108.72	\$1,108.72
Schmitz, Ronald	12/01/2021	12/02/2021	Washington, D.C.		Visit VRS Investment Property - Catholic University	-	\$367.88	\$367.88
Alouf, John	12/13/2021	12/13/2021	New York, NY		Due diligence/on-site visit with Veritas	-	\$865.20	\$865.20
Coleman, Thomas	02/23/2022	02/24/2022	Toronto, Canada		Sprott - Due Diligence	-	\$1,084.78	\$1,084.78

Detail of Travel Related Expenses
Virginia Retirement System
Board/Committee Members and Selected VRS Staff
Paid in Q3 2022

Traveler	Travel Start	Travel End	Destination	Sponsor	Purpose	Sponsor Paid	VRS Paid	Total
Gentry III, William	03/21/2022	03/23/2022	Miami, FL		Travel to Miami for meeting with Trivest Partners , Thoma Bravo Annual Meeting and Due Diligence	-	\$1,547.94	\$1,547.94
Matoua, Katherine	12/05/2021	12/10/2021	Charlottesville VA		Attend VCU CMG Commonwealth Management Institute in Charlottesville, Va	-	\$2,759.81	\$2,759.81
Murphy, James	11/17/2021	11/18/2021	New York, NY		On-Site Meeting with Siris Partners / Due Diligence	-	\$539.99	\$539.99
Total						-	\$11,105.78	\$11,105.78

**VRS BOARD OF TRUSTEES AND COMMITTEES
RECORD OF ATTENDANCE & PER DIEMS
FOR 1Q2022**

Member	Area	Month Paid:			Total Days Attended	Per Diem Rate	Per Diem Payments			Total
		Feb-22					Jan	Feb	Mar	
		2/8/22	2/9/22	2/10/22						
A&P	B&A	BOT								
J BRANDON BELL, II	BOT	-	X	X	2	\$ 300.00	\$ -	\$ 600.00	\$ -	\$ 600.00
JOHN M. BENNETT	BOT	X	X	X	3	300.00	-	900.00	-	900.00
MICHAEL P. DISHAROON	BOT	-	X	X	2	300.00	-	600.00	-	600.00
WILLIAM A. GARRETT	BOT	-	X	X	2	300.00	-	600.00	-	600.00
SUSAN GOODEN	BOT	-	-	X	1	300.00	-	300.00	-	300.00
W. BRETT HAYES	BOT	X	-	X	2	300.00	-	600.00	-	600.00
O'KELLY E. MCWILLIAMS, III	BOT	X	X	X	3	300.00	-	900.00	-	900.00
JOSEPH W. MONTGOMERY	BOT	X	X	X	3	300.00	-	900.00	-	900.00
TROILEN G. SEWARD	BOT	X	X	X	3	300.00	-	900.00	-	900.00
RIVINDRA DEO	DCPAC	-	-	-	-	300.00	-	-	-	-
SHANNON T. IRVIN	DCPAC	-	-	-	-	300.00	-	-	-	-
RICK LARSON	DCPAC	-	-	-	-	300.00	-	-	-	-
BRENDA O. MADDEN	DCPAC	-	-	-	-	300.00	-	-	-	-
ARUN MURALIDHAR (1)	DCPAC	-	-	-	-	300.00	-	-	-	-
EDWARD N. SMITHER	DCPAC	-	-	-	-	300.00	-	-	-	-
DAVID A. WINTER	DCPAC	-	-	-	-	300.00	-	-	-	-
DEBORAH ALLEN-HEWITT	IAC	-	-	-	-	300.00	-	-	-	-
MICHAEL R. BEASLEY	IAC	-	-	-	-	300.00	-	-	-	-
THEODORE ECONOMOU	IAC	-	-	-	-	-	-	-	-	-
THOMAS S.GAYNER	IAC	-	-	-	-	300.00	-	-	-	-
LAWRENCE E KOCHARD	IAC	-	-	-	-	300.00	-	-	-	-
NANCY G. LEAKE	IAC	-	-	-	-	300.00	-	-	-	-
WILBERT BRYAN LEWIS	IAC	-	-	-	-	300.00	-	-	-	-
ROD SMYTH	IAC	-	-	-	-	300.00	-	-	-	-
WILLIAM H. WEST	IAC	-	-	-	-	300.00	-	-	-	-
							\$ -	\$ 6,300.00	\$ -	\$ 6,300.00

Number Attending	5	7	9	21				
Total Days per Diem Paid (Control Total)	5	7	9	21	x \$300	=		6,300.00

(1) Appointed to DCPAC effective 2/10/22

X = Present