COMMONWEALTH of VIRGINIA

SHARON H. LAWRENCE, CPA, CGMA
ACTING COMPTROLLER

Office of the Comptroller

P. O. BOX 1971
RICHMOND, VIRGINIA 23218-1971

March 11, 2024

Department of Health and Human Services
Office of Inspector General
Office of Audit Services
National External Audit Review Center
1100 Walnut Street, Suite 850
Kansas City, MO 64106

To Whom It May Concern:

In addition to promptly taking corrective action on all findings, in accordance with CFR §200.511 Audit findings follow-up (c) *Corrective action plan*, the State Comptroller of Virginia (auditee) has prepared, in a document separate from the auditor's findings described in CFR §200.516 Audit findings, a corrective action plan to address each audit finding included in the current year auditor's report. The corrective action plan also cites findings relating to the financial statements, which are required to be reported in accordance with *Generally Accepted Government Auditing Standards*. The corrective action plan cites the reference number the auditor assigned to each auditing finding, name(s) of the contact person(s) responsible for corrective action, the corrective action planned, and the anticipated completion date. The corrective action plan does not express a disagreement with any of the audit findings nor does it disclose that corrective action is not required.

Certain corrective actions planned are not contained in this corrective action plan because they contain descriptions of security mechanisms and are Freedom of Information Act Exempt under §2.2-3705.2 of the *Code of Virginia*. Federal awarding agencies or pass-through entities needing such information in formulating their management decisions as required by CFR §200.521 Management decision, should communicate with the contact person responsible for the respective corrective action planned to address the audit finding.

The Commonwealth of Virginia Single Audit Report for the Year Ended June 30, 2023 containing all findings can be found at www.apa.virginia.gov or is available from the Federal Audit Clearinghouse web site. If you have any questions, please contact our office at (804) 371-8912.

Sincerely,

Sharon H. Lawrence

Sharon H. Lawrence

COMMONWEALTH OF VIRGINIA
Corrective Action Plan
For the Year Ended June 30, 2023

Audit Finding Reference Number	Responsible Person(s) Corrective Action Planned Estimated Completion Date
Strengthen Controls over Financial Reporting 2023-001 DHRM	Responsible Contact Person(s): Denise Sandlin, Chief Financial Officer Donna Brown, Finance Officer Corrective Action Planned: Finance hired a new Chief Financial Officer at the end of FY2023. The Accounting Specialist position was reclassified to a Financial Analyst position and DHRM will cross train the Financial Analyst. There are all new employees in the finance department. Desk procedures are being written and there is more than one reviewer on all attachments and supplemental documents. Estimated Completion Date: 6/30/2024
Improve Controls over GASB Statement No. 75 Financial Information Review 2023-002 DHRM	Responsible Contact Person(s): Denise Sandlin, Chief Financial Officer Donna Brown, Finance Officer Corrective Action Planned: Finance hired a new CFO at the end of FY2023. The Accounting Specialist position was reclassified to a Financial Analyst position. There are all new employees in the finance department. DHRM is working on the completion of desk procedures. There is more than one reviewer on the GASB process and DHRM is cross training the Financial Analyst to allow ample time to eliminate errors. DHRM has requested to receive earlier drafts from the contractor to allow ample time to review and prepare the final submission. Estimated Completion Date: 6/30/2024
Improve Controls over Identifying, Tracking, Recording, and Reporting Right-to-Use Assets 2023-003 VITA	Responsible Contact Person(s): Cynthia Cordova-Edwards, Chief Information Officer Corrective Action Planned: In continued consultation with APA and others, VITA will also use the business judgment that GASB standards allow in application to VITA's multiple component contracts. VITA will seek additional contracted resources while continuing to advance implementation of GASB 87/96 along with acquiring and building internal talent. VITA will also seek to improve financial information and reporting systems to meet the requirements of GASB 87/96. (VITA's legacy financial system is over 20 years old and no longer meets the needs of modern financial reporting.) VITA will request funding through the budgetary process for improvements to its financial management applications and requisite staffing. VITA will continue working with DOA to ensure application of the GASB requirements is as needed for ACFR reporting. To the extent APA believes such corrective actions are incomplete, VITA will continue to implement previously reported corrective actions: 1. Identify the complete population of leases for which VITA has a reporting obligation. 2. Consistently determine the lease term and asset grouping of the leases across all contracts. 3. Determine VITA's incremental borrowing rate for leased assets. 4. Document and retain the reconciliation process for verifying and ensuring the completeness and accuracy of leased asset data provided for use in valuing VITA's lease assets and liabilities. 5. Implement policies and procedures to ensure consistent application across contracts for which VITA has a reporting obligation. 6. Appropriately review and report contracts within reporting scope for GASB 87. Estimated Completion Date: 12/31/2024
Improve Internal Controls over Financial Reporting of Leases under GASB Statement No. 87 2023-004 DGS	Responsible Contact Person(s): Sara Page, Controller Mike Nolan, Director of Real Estate Services Corrective Action Planned: DGS is in the process of hiring a consultant to assist with the assessment of policies and procedures for financial reporting of leases under GASB 87. Estimated Completion Date: 6/30/2025
Strengthen Controls over Financial Reporting 2023-005 VDH	Responsible Contact Person(s): Carla Green, Director of Financial Management Corrective Action Planned: Management has prioritized the filling of vacancies in the Office of Financial Management to ensure sufficient resources are available for financial oversight and reporting. Estimated Completion Date: 6/30/2024
Improve Controls over Journal Entries 2023-006 VDH	Responsible Contact Person(s): Carla Green, Director of Financial Management Corrective Action Planned: Management has prioritized the filling of vacancies in the Office of Financial Management to ensure sufficient resources are available for financial oversight. Additionally, the Office of Financial Management is reviewing system access and permissions, including another layer of personnel to review journal entries before final approval. Estimated Completion Date: 4/30/2024
Improve Governance Structure and Resources Surrounding Financial Reporting Process 2023-007 UVA	Responsible Contact Person(s): Jennifer Wagner-Davis, Executive Vice President and Chief Operating Officer Chief Executive Officer UVA Health, UVA Finance, and Medical Center Controller's Office Corrective Action Planned: UVA will continue to implement a combination of improved business processes and future reporting enhancements focused more on technical and operational presentation of respective, and consolidated, GAAP statements. These will include detective controls and analysis of UVA's respective close processes, more frequent reconciliations, as well as additional review and verification of statement presentation to the Auditor of Public Accounts. It is important to reiterate that both Medical Center and the Consolidated statements undergo separate audits from the APA, with Medical Center and the Academic Division operating as separate state agencies – both of which are material to the Consolidated Statements. Current and Ongoing: The University will continue to meet monthly with leadership to provide updates on all related aspects of UVA financial reporting environment. The collective management team will also update the President and Audit Chair bi-monthly or more often as needed. In addition, UVA will continue to use third party expertise and external audits for its component units including Community Health, as well as for technical assistance on new Government Accounting Standard Board adoption and actuarial support. Lastly, continued recruitment of professionals to ensure full staffing at both the Medical Center and Academic accounting and reporting teams will be ongoing as vacancies may arise. The University will continue to meet regularly with the APA in preparation for, and during, the FY2024 audit. Moving forward, APA status meetings will occur for the Academic Division, Medical Center Division, and the Consolidated team jointly, along with any other relevant parties. Immediate Corrective Action: The University will immediately begin planning for all year end statement preparation procedures as well as the overall consolidation process, including but not limited to, duties and responsibilities, testing and review protocols, additional review and detective controls, quality assurance measures, and potential realignment or personnel enhancements that can increase or improve the overall reporting and control environment. This plan will be reviewed by the Audit Chair and President on or before March 2024. The Board of Visitors was updated regarding the status of this management point in the December 7th Audit Committee. Leadership will finalize a remediation plan and share with the APA and the Audit Committee of the Board of Visitors no later than January 2024. Estimated Completion Date: 6/30/2024

Audit Finding Reference Number	Responsible Person(s) Corrective Action Planned Estimated Completion Date
Strengthen Internal Controls over Financial Reporting of Non-Reimbursement Grants 2023-008 DSS	Responsible Contact Person(s): Ida Witherspoon, Chief Financial Officer Paige Elswick, Controller Corrective Action Planned: DSS will develop and implement procedures outlining its process for preparing the Attachment 27 submission. Additionally, DSS will perform a thorough review of its Attachment 27 submission before submitting it to the Department of Accounts. Estimated Completion Date: 6/30/2024
Continue to Improve Controls over the Calculation of Contractual Commitments 2023-009 DBHDS	Responsible Contact Person(s): Nathan Miles, Chief Financial Officer Corrective Action Planned: The Office of the Comptroller is nearing completion of more detailed written procedures in this area. The procedures will detail the calculation and the controls to ensure reasonableness. Estimated Completion Date: 3/31/2024
Improve Information Security Program and Controls 2023-010 DMAS	Responsible Contact Person(s): Steve Hanoka, Chief Information Security Officer Corrective Action Planned: Policies are reviewed and signed. Procedures are in progress, to be followed by implementation. DMAS wants to meet with the APA and VITA to discuss Pen Test and vulnerability scan processes. Completion of System Security Plans (SSPs) are about 50% complete, with 6 SSPs complete, 3 under review, 1 in draft and 7 to schedule. A program management policy/standard has been written and is under review. Estimated Completion Date: 4/1/2024
Improve Database Security 2023-011 DOA	Responsible Contact Person(s): Stacy McCracken, Director - Enterprise Applications Office Quinton Litchford, Chief Information Officer Corrective Action Planned: This finding was marked as FOIA Exempt (FOIAE) and as a result, the State Comptroller has determined that the resulting corrective actions are FOIAE under §2.2-3705.2 (9.) of the Code of Virginia. Federal awarding agencies and pass-through entities, please see the Appendix titled “Applicable Management Contacts for Findings and Questioned Costs” to request the corrective action planned from the applicable entity. Estimated Completion Date: 5/31/2024
Improve Database Security 2023-012 VRS	Responsible Contact Person(s): Mark Rein, Chief Technology & Security Officer Corrective Action Planned: This finding was marked as FOIA Exempt (FOIAE) and as a result, the State Comptroller has determined that the resulting corrective actions are FOIAE under §2.2-3705.2 (9.) of the Code of Virginia. Federal awarding agencies and pass-through entities, please see the Appendix titled “Applicable Management Contacts for Findings and Questioned Costs” to request the corrective action planned from the applicable entity. Estimated Completion Date: 3/31/2024
Improve IT Risk Management and Contingency Planning Documentation 2023-013 DPB	Responsible Contact Person(s): Michelle Vucci, Associate Director - Administrative Services Corrective Action Planned: Agency is actively addressing issues identified by the auditor and is working with the Virginia Information Technologies Agency (VITA) to remediate weaknesses. Estimated Completion Date: 12/31/2024
Continue Improving IT Risk Management Program 2023-014 DSS	Responsible Contact Person(s): Barry Davis, Chief Information Security Officer and Director of Information Security & Risk Management Kevin Platea, Chief Information Officer Corrective Action Planned: To improve the governance structure of the agency, ISRM Division Leadership is working with a vendor to address the division’s responsibility around defining and communicating the Security and Risk Management program. The goal is to educate the agency System Owners, Data Owners, System Administrators, System User, and Data Custodians as to their roles and responsibilities in managing risk associated with agency data and systems. The Division of ISRM will deliver System Owner training to the Agency Executive Team in April in support of the Commonwealth’s requirement that System Owner’s manage risks associated with their systems. This training will also highlight the importance of Configuration Management and Software and Service Acquisition. The Division of ISRM will also construct and offer training on Configuration Management and Software and Service Acquisition to whichever resources the Agency identifies to own such related processes. The training will be ready to be provided no later than August 1, 2023. Estimated Completion Date: 12/31/2023
Improve Web Application Security 2023-015 DSS	Responsible Contact Person(s): Kevin Platea, Chief Information Officer Corrective Action Planned: This finding was marked as FOIA Exempt (FOIAE) and as a result, the State Comptroller has determined that the resulting corrective actions are FOIAE under §2.2-3705.2 (9.) of the Code of Virginia. Federal awarding agencies and pass-through entities, please see the Appendix titled “Applicable Management Contacts for Findings and Questioned Costs” to request the corrective action planned from the applicable entity. Estimated Completion Date: 12/31/2024
Continue to Improve Database Security 2023-016 DBHDS	Responsible Contact Person(s): Russell Accashian, Chief Information Officer Corrective Action Planned: This finding was marked as FOIA Exempt (FOIAE) and as a result, the State Comptroller has determined that the resulting corrective actions are FOIAE under §2.2-3705.2 (9.) of the Code of Virginia. Federal awarding agencies and pass-through entities, please see the Appendix titled “Applicable Management Contacts for Findings and Questioned Costs” to request the corrective action planned from the applicable entity. Estimated Completion Date: 12/31/2024

Audit Finding Reference Number	Responsible Person(s) Corrective Action Planned Estimated Completion Date
Conduct Information Technology Security Audits 2023-017 VDH	Responsible Contact Person(s): Tasha Owens, Director of Internal Audit Corrective Action Planned: The Office of Internal Audit (OIA) has completed its recruitment of two IT Auditor positions (Senior IT Auditor and Staff IT Auditor) as of January 10, 2024. OIA is developing a formal process for conducting IT audits over each sensitive system at least every three years. First, OIA is working with Office of Information Management and Information Security Officer to identify the sensitive systems at VDH. Second, the Director of Internal Audit will determine which IT audits will be included on the FY25 Audit Plan using a risk-based methodology. Two internal audits are currently in progress as of February 29, 2024. OIA has contracted with a third party to conduct four IT audits by June 30, 2024. Applicable Deliverables: FY25 Audit Plan with IT sensitive audits. Estimated Completion Date: 6/30/2025
Improve Database Security 2023-018 DMV	Responsible Contact Person(s): Beau Hurley, Chief Information Security & Agency Risk Management Corrective Action Planned: This finding was marked as FOIA Exempt (FOIAE) and as a result, the State Comptroller has determined that the resulting corrective actions are FOIAE under §2.2-3705.2 (9.) of the Code of Virginia. Federal awarding agencies and pass-through entities, please see the Appendix titled "Applicable Management Contacts for Findings and Questioned Costs" to request the corrective action planned from the applicable entity. Estimated Completion Date: 12/31/2024
Improve Database Security 2023-019 VDOT	Responsible Contact Person(s): Lynn Hadden, Information Technology Division - Division Administrator Corrective Action Planned: This finding was marked as FOIA Exempt (FOIAE) and as a result, the State Comptroller has determined that the resulting corrective actions are FOIAE under §2.2-3705.2 (9.) of the Code of Virginia. Federal awarding agencies and pass-through entities, please see the Appendix titled "Applicable Management Contacts for Findings and Questioned Costs" to request the corrective action planned from the applicable entity. Estimated Completion Date: 12/31/2024
Conduct IT Risk Assessments and Develop System Security Plans 2023-020 VDOT	Responsible Contact Person(s): Andrew Green, Information Security Officer - Information Security Division Corrective Action Planned: 1. Bring the Risk Assessment Plan to a current status by June 30, 2024. 2. Complete new risk assessment and system security plan for all sensitive systems by December 31, 2024. 3. Issue new Risk Assessment policy by September 30, 2024. Estimated Completion Date: 12/31/2024
Improve IT Risk Management and Contingency Planning Program 2023-021 DHRM	Responsible Contact Person(s): Antonio Villafana, Chief Information Officer Blechior Mira, Information Security Officer Corrective Action Planned: DHRM is in the process writing a Disaster Recovery Plan(DRP) based on DHRM COOP recovery times. Estimated Completion Date: 6/30/2024
Improve IT Risk Management Program 2023-022 DOE/DAPE	Responsible Contact Person(s): Diane Carnohan, Chief Information Security Officer Corrective Action Planned: This finding was marked as FOIA Exempt (FOIAE) and as a result, the State Comptroller has determined that the resulting corrective actions are FOIAE under §2.2-3705.2 (9.) of the Code of Virginia. Federal awarding agencies and pass-through entities, please see the Appendix titled "Applicable Management Contacts for Findings and Questioned Costs" to request the corrective action planned from the applicable entity. Estimated Completion Date: 12/31/2024
Improve IT Risk Management Program and Contingency Planning 2023-023 VCSP	Responsible Contact Person(s): Rosario Igharas, Director of Information Security Corrective Action Planned: This finding was marked as FOIA Exempt (FOIAE) and as a result, the State Comptroller has determined that the resulting corrective actions are FOIAE under §2.2-3705.2 (9.) of the Code of Virginia. Federal awarding agencies and pass-through entities, please see the Appendix titled "Applicable Management Contacts for Findings and Questioned Costs" to request the corrective action planned from the applicable entity. Estimated Completion Date: 9/30/2024
Improve IT Risk Management and Contingency Planning 2023-024 ABC	Responsible Contact Person(s): Diane Enroughty, Information Security Governance Risk & Compliance Manager - Information Security Officer Corrective Action Planned: The noted findings are mostly about a backlog and timely update in ABC's process documentation, largely caused by staff turnover. As most of ABC's critical systems are relatively new and fully assessed during acquisition and implementation, IT will work with a third-party vendor to schedule systems review during the next fiscal year to reduce the backlog. ABC's systems are now mostly separate components that can operate independently. During the year, many of these presented challenges, but ABC successfully recovered these systems as part of its routine system support. ABC will work with its vendor for a documentation standard to meet the requirement for documenting testing of component results within the IT system portfolio and conduct simulated tests of critical systems where there have been no exceptions to document. The Enforcement division is also planning a tabletop business continuity exercise this year in which IT will participate. Estimated Completion Date: 6/30/2024
Improve Database Security 2023-025 VAL	Responsible Contact Person(s): Paul Battle, Director of Information Security Corrective Action Planned: This finding was marked as FOIA Exempt (FOIAE) and as a result, the State Comptroller has determined that the resulting corrective actions are FOIAE under §2.2-3705.2 (9.) of the Code of Virginia. Federal awarding agencies and pass-through entities, please see the Appendix titled "Applicable Management Contacts for Findings and Questioned Costs" to request the corrective action planned from the applicable entity. Estimated Completion Date: 5/1/2024

Audit Finding Reference Number	Responsible Person(s) Corrective Action Planned Estimated Completion Date
Improve Database Security 2023-026 UVA/AD	Responsible Contact Person(s): Kelly Donney, Chief Information Officer Dana German, Deputy Chief Information Officer Jason Belford, Chief Information Security Officer Corrective Action Planned: This finding was marked as FOIA Exempt (FOIAE) and as a result, the State Comptroller has determined that the resulting corrective actions are FOIAE under §2.2-3705.2 (9.) of the Code of Virginia. Federal awarding agencies and pass-through entities, please see the Appendix titled "Applicable Management Contacts for Findings and Questioned Costs" to request the corrective action planned from the applicable entity. Estimated Completion Date: 12/31/2023
Improve Information Security Program and IT Governance 2023-027 DSS	Responsible Contact Person(s): Barry Davis, Chief Information Security Officer and Information Security & Risk Management Kevin Platea, Chief Information Officer Corrective Action Planned: This finding was marked as FOIA Exempt (FOIAE) and as a result, the State Comptroller has determined that the resulting corrective actions are FOIAE under §2.2-3705.2 (9.) of the Code of Virginia. Federal awarding agencies and pass-through entities, please see the Appendix titled "Applicable Management Contacts for Findings and Questioned Costs" to request the corrective action planned from the applicable entity. Estimated Completion Date: 12/31/2023
Continue Dedicating Resources to Support Information Security Program 2023-028 DBHDS	Responsible Contact Person(s): Glenn Schmitz, Chief Information Security Officer Corrective Action Planned: The Security Office is focusing resources from future project support and will require contractor ISO support for all new projects. Estimated Completion Date: 12/31/2024
Allocate Resources to Enforce Separation of Duties 2023-029 DPB	Responsible Contact Person(s): Michelle Vucci, Associate Director - Administrative Services Corrective Action Planned: After this finding was first shared with DPB, the agency made internal policy and system changes to address this finding. Estimated Completion Date: 1/31/2024
Complete Annual Review over User Access to University Information Systems 2023-030 UVA/AD	Responsible Contact Person(s): Stephen Farmer, Vice Provost for Enrollment Corrective Action Planned: University policy allows two options for reviewing user access to major systems. One option is to implement a business process that immediately/automatically removes access when an individual leaves their position; assures ongoing segregation of duties; and monitors for and addresses potential instances of misuse. Since 2012, the University has had a process for immediately deprovisioning access to the system when an employee leaves the University or changes roles within the University. When new users request access, the data stewards ensure there is adequate segregation of duties before granting approval. The second option for reviewing user access is to administer a process at least annually to review and reauthorize or revoke user privileges providing access to highly sensitive data or elevated system privileges. The University completed a test of the new system tool with the University Registrar in fall 2022 (FY23). In February 2023, the University updated policy for conducting its review of major systems. Human Resources and Finance planned for and completed their review in June 2023. The review of the system could not be conducted concurrently with Human Resources and Finance due to system limitations and resource constraints. The University's intent was to identify best practices from the Human Resources and Finance review; those lessons learned have been shared both from a user perspective and an information technology perspective for the system attestation. The system attestation is scheduled for spring 2024 and will be completed no later than June 30, 2024. Estimated Completion Date: 6/30/2024
Complete Annual User Access Reviews 2023-031 UVAH	Responsible Contact Person(s): Amy Karr, Health System Technology Services Corrective Action Planned: Monthly reminders are shared with any Manager/Supervisor whose access review is outstanding. Beginning in July 2023, the UVA Health Information Security Officer started sending out quarterly follow up reminders to any Supervisor/Manager whose annual Supervisor Review remains incomplete. Starting in October 2023, Supervisors/Managers who remain non-compliant after the quarterly notification will be escalated to more senior leadership (Chief or Dean) to ensure completion of their review; any outstanding access will then be terminated. Significant improvements are expected after this quarterly escalation. UVAH has continued to stabilize and strengthen the process within the next two quarterly cycles and tighten the timeline for review, escalation, and access termination (as appropriate). Estimated Completion Date: 4/30/2024
Continue to Implement Compliant Application Access Management Procedures 2023-032 DBHDS	Responsible Contact Person(s): Glenn Schmitz, Chief Information Security Officer Corrective Action Planned: In FY25 the Security Office will be allocating funds to bring on a dedicated SSO contractor to review and work with all application owners and 3rd party SaaS solution vendors to configure the applications to be SSO compliant with identity access management platform. Due to the number of applications in the inventory, this effort is estimated to take approximately 3 years to complete. Estimated Completion Date: 12/31/2027
Improve Documentation for Separation of Duty Conflicts 2023-033 DSS	Responsible Contact Person(s): Ida Witherspoon, Chief Financial Officer Corrective Action Planned: Update the financial systems access policy to require written documentation to justify conflicting access. Estimated Completion Date: 12/31/2023
Evaluate Separation of Duty Conflicts within the Case Management System 2023-034 DSS	Responsible Contact Person(s): Angela Morse, Director of Benefit Programs Kavansa Gardner, Information Technology Manager Corrective Action Planned: DSS will perform and document a conflicting access review for the case management system to identify the combinations of roles that could pose separation of duties conflicts and ensure compensating controls are in place to mitigate risks arising from those conflicts. Additionally, DSS will work with a vendor to update the role-based security access documentation to reflect all system changes from prior case management system related releases when there are proposed changes to the roles matrix. Estimated Completion Date: 12/31/2024

Audit Finding Reference Number	Responsible Person(s) Corrective Action Planned Estimated Completion Date
Perform Annual Review of Case Management System Access 2023-035 DSS	Responsible Contact Person(s): Barry Davis, Chief Information Security Officer and Director of Information Security & Risk Management Steve McCauley, Assistant Division Director Corrective Action Planned: DSS will perform an annual access review of user accounts for the case management system. Estimated Completion Date: 12/31/2024
Perform Annual System Access Reviews 2023-036 DMAS	Responsible Contact Person(s): Mike Jones, Chief Information Officer Steve Hanoka, Chief Information Security Officer Corrective Action Planned: The 2023 Annual Access Review for the claims processing system through secure web application surveys began in the 4th Quarter 2023. Three separate surveys were sent to perform access review for DSS, Contractor and DMAS Internal access review. • DSS annual review sent on November 9, 2023 and ended on November 20, 2023 • Contractor review sent on November 30, 2023 and ended on December 15, 2023 • DMAS review sent on December 15, 2023 and ended on January 13, 2024 All 3 surveys requested managers to review their employees access and confirm if it was required or if the access should be revoked. Survey results are available to perform follow up actions. DMAS Security is currently reviewing the survey results and revoking access where requested. Estimated Completion Date: 6/30/2024
Improve System Access Procedures 2023-037 VDH	Responsible Contact Person(s): Suresh Soundararajan, Chief Information Officer Othello Dixon, Acting Information Security Officer Corrective Action Planned: The Corrective Action for this finding contains sensitive system information and has been redacted to protect the system owner from vulnerabilities. Federal awarding agencies and pass-through entities, please see the Appendix titled "Applicable Management Contacts for Findings and Questioned Costs" to request the corrective action planned from the applicable entity. Estimated Completion Date: 10/31/2024
Implement a Process to Annually Review User Access 2023-038 DMV	Responsible Contact Person(s): Beau Hurley, Chief Information Security & Agency Risk Management Corrective Action Planned: The Department of Motor Vehicles has started the annual review using the new process and will include this in DMV start of the year tasks. Estimated Completion Date: 10/31/2024
Improve System Access Policies and Procedures for Critical Systems 2023-039 VAL	Responsible Contact Person(s): Paul Battle, Director of Information Security Corrective Action Planned: Lottery will update the system access control policy incorporated into the Information Security Program, document critical roles and privileges and formally document internal processes/procedures for the critical systems identified. Estimated Completion Date: 3/31/2024
Improve Management of Access to the Retirement Benefits System 2023-040 DOC/CA	Responsible Contact Person(s): Lucinda R. Childs-White, Human Resources Director Corrective Action Planned: 1. Human Resource Director Memorandum will be distributed to Organizational Unit Heads, Human Resource Officers, and Payroll Leadership outlining the expectations for prompt notification of separations to the System Administrator. 2. The expectations for prompt notification of systems access removal has been discussed and will be reinforced through future Statewide HR Staff Meetings. 3. The designated system Security Administrator will conduct semi-annual reconciliations of the human capital management system separations, reconciling system access permissions. Estimated Completion Date: 7/1/2024
Improve Offboarding Process 2023-041 VDOT	Responsible Contact Person(s): Mary-Margaret Allen, Human Resources Division - Division Administrator Corrective Action Planned: 1. Improve system functionality and re-engineer the offboarding process to streamline certain tasks through system notification. 2. Communicate the importance and requirement that supervisors complete separation checklists. Ensure access removal within 24 hours. 3.Update or develop training materials and job aids on the separation checklist process. Provide training to supervisors on separation checklists. Estimated Completion Date: 9/30/2024
Continue Strengthening the System Access Removal Process 2023-042 VDH	Responsible Contact Person(s): Suresh Soundararajan, Chief Information Officer Twinkle Oliver, Director of Human Resources Corrective Action Planned: VDH OIM staff will review the Staff Separation process and make improvements. VDH is always seeking ways to improve, and for the content management system, VDH has added a single sign-on feature, which is in the testing phase now. It will be in production by the middle of March. This all should enhance timely system access removal. Additionally, ISO gets an email from HR for immediate termination, and ISO terminates the employee using identity access management software. Finally, ISO will start the Identity Access Review campaign for the content management system next week. Implementation Time for Single Sign-on: March 9, 2024. Estimated Completion Date: 12/31/2024
Monitor Internal Controls to Ensure Timely Removal of System Access 2023-043 DSS	Responsible Contact Person(s): Barry Davis, Chief Information Security Officer and Director of Information Security & Risk Management Melinda Raines, Director of Human Resources Karen Holt, Human Resources Business Process Consultant Corrective Action Planned: An agency-wide work group will be established to determine the exact processes need to implement the controls necessary to address this finding. HR and ISRM have identified the need for new reporting and interfaces to regain compliance. DSS had deployed DOA human capital management system and an internal system that will need to have interfaces developed. Estimated Completion Date: 6/30/2024

Audit Finding Reference Number	Responsible Person(s) Corrective Action Planned Estimated Completion Date
Revoke Systems Access For Separated Employees in a Timely Manner 2023-044 TAX	Responsible Contact Person(s): Karen Doty, Human Resources Director Corrective Action Planned: The Human Resources Director will remind supervisors of the importance of the timely revocation of systems access for separated employees. Additionally, the Employee Separation Checklist will be revised so that responsible supervisors are instructed to enter the revocation of systems access upon the notice of separation rather than the actual separation. Estimated Completion Date: 3/31/2024
Improve IT Change Control and Configuration Management Process 2023-045 VRS	Responsible Contact Person(s): Mark Rein, Chief Technology & Security Officer Corrective Action Planned: Develop change management operating procedures and implement change management software. Estimated Completion Date: 12/31/2024
Continue to Improve IT Change and Configuration Management Policy and Process 2023-046 DPB	Responsible Contact Person(s): Michelle Vucci, Associate Director - Administrative Services Corrective Action Planned: After this finding was first shared with DPB, the agency made internal policy and system changes to address this finding. Estimated Completion Date: 1/31/2024
Develop Baseline Configurations for Information Systems 2023-047 DBHDS	Responsible Contact Person(s): Glenn Schmitz, Chief Information Security Officer Corrective Action Planned: The Security Office has instituted the BIA Process to review all applications in the inventory. Part of this process is to create, review, and approve baseline configurations of the application. Due to the current number of applications in the inventory, resource constraints, and competing priorities, this effort will take approximately 3 years to fully complete as part of the standard 3 year BIA certification process. Estimated Completion Date: 12/31/2027
Improve Change Management Process for Information Technology Environment 2023-048 DBHDS	Responsible Contact Person(s): Russell Accashian, Chief Information Officer Corrective Action Planned: IT Change Management improvements that have been implemented include the following: documented CAB agendas, minutes, inclusion of additional representation such as Enterprise Applications, Enterprise Project Management Office, and VITA to present changes from their respective areas for CAB approval. Improvements in progress: Hiring of a Change Manager to facilitate and make continuous improvements. Estimated Completion Date: 12/31/2024
Continue Improving IT Change and Configuration Management Process 2023-049 DSS	Responsible Contact Person(s): Kevin Platea, Chief Information Officer Corrective Action Planned: This finding was marked as FOIA Exempt (FOIAE) and as a result, the State Comptroller has determined that the resulting corrective actions are FOIAE under §2.2-3705.2 (9.) of the Code of Virginia. Federal awarding agencies and pass-through entities, please see the Appendix titled “Applicable Management Contacts for Findings and Questioned Costs” to request the corrective action planned from the applicable entity. Estimated Completion Date: 6/30/2024
Improve Change Control Process 2023-050 VDOT	Responsible Contact Person(s): Lynn Hadden, Information Technology Division - Division Administrator Corrective Action Planned: This finding was marked as FOIA Exempt (FOIAE) and as a result, the State Comptroller has determined that the resulting corrective actions are FOIAE under §2.2-3705.2 (9.) of the Code of Virginia. Federal awarding agencies and pass-through entities, please see the Appendix titled “Applicable Management Contacts for Findings and Questioned Costs” to request the corrective action planned from the applicable entity. Estimated Completion Date: 8/31/2024
Improve change Control Process 2023-051 VEC	Responsible Contact Person(s): David Clark, Information Security Officer Corrective Action Planned: The Information Security Unit has documented a process for the types of changes that trigger a security impact analysis (SIA) as well as a request form for a security impact review. Part of the SIA process will be to determine if pre-implementation testing is required. The Information Security Unit will retain documentation in accordance with the Configuration Management Policy. Once the processes are further defined, the Information Security Unit will update the Configuration Management Policy & Procedures. Estimated Completion Date: 3/31/2024
Improve Monroe IT Change and Configuration Management Process 2023-052 DOA	Responsible Contact Person(s): Quinton Litchford, Chief Information Officer Corrective Action Planned: Monroe IT has implemented a Security Impact Analysis in its change management process effective January 1, 2024. All coding changes require that a developer complete and upload a Security Impact Analysis for every Request Tracking System (RTS) item. The ISO must review and approve the Security Impact Analysis before the change can be promoted to the production environment. Most server configuration management RTS items follow the same process, with the exception of "standard changes" which require a yearly Security Impact Analysis that covers a set of repeatable changes. Standard Changes continue to follow the change management process, but the Security Impact Analysis process in RTS defers to the existing approved Security Impact Analysis. An example of a Standard Change would be the renewal and installation of SSL certificates for websites. Estimated Completion Date: 1/1/2024
Conduct Timely IT Security Audits 2023-053 DOA	Responsible Contact Person(s): Stacy McCracken, Director - Enterprise Applications Office Quinton Litchford, Chief Information Officer Corrective Action Planned: The agency has contracted with an approved vendor to perform an audit for the impacted system. The audit is underway and the Final Audit Report is expected to be completed in early April of 2024. DOA has confirmed with VITA's Auditing Service that the impacted system is on the audit schedule for calendar year 2025. Estimated Completion Date: 4/30/2024

Audit Finding Reference Number	Responsible Person(s) Corrective Action Planned Estimated Completion Date
Conduct Information Technology Security Audits over Sensitive Systems 2023-054 DBHDS	Responsible Contact Person(s): Divya Mehta, Director of Internal Audit Corrective Action Planned: There has been turnover in the only IT Auditor role Internal Audit has. That position has been filled as of August 10, 2023. DBHDS is continuing to work on planned audits this year, with 2 of 5 facilities on the audit plan already completed, and two in-progress. Due to an extremely high per hour cost of contracting these services along with the volume of systems to be audited, DBHDS didn't think it was cost effective to contract these audit services out. Another attributing factor is the volatility in the number of sensitive systems. As of December 5, 2023 plan, number of sensitive systems requiring an IT Security Audit is reduced which may again change within next few months. DBHDS keeps coming across systems that are not in use however not retired. Due to these changes, it has been difficult to assess the number of positions needed to complete these audits. DBHDS will continue to work with CO and facilities to reduce the number of agency sensitive systems, work collaboratively with IT and Security to retire systems not in use and will hire additional staff based on the need. Estimated Completion Date: 12/31/2024
Obtain and Review Information Security Audit 2023-055 DMAS	Responsible Contact Person(s): Mike Jones, Chief Information Officer Corrective Action Planned: The vendor started the security audit in September 2023 and completed in December 2023. The report was sent to DMAS in February 2024. Next steps- The report needs to be reviewed and the Contract Administrator will work with the vendor to ensure Plan of Action and Milestones (POAMs) are completed to address the risks and control gaps. The Contract Administrator will monitor the vendor to ensure the vendor meets to terms of the contract and submits a security audit every two years. Estimated Completion Date: 6/30/2024
Conduct Information Technology Security Audits 2023-056 DSS	Responsible Contact Person(s): Barry Davis, Chief Information Security Officer and Director of Information Security & Risk Management John Vosper, Information Technology Audit Manager Corrective Action Planned: DSS has contracted with a contractor to perform IT audits once every three years on an ongoing rotating basis. Estimated Completion Date: 12/31/2023
Conduct Timely IT Security Audits 2023-057 DMV	Responsible Contact Person(s): Diane Shember, Director of Internal Audit (Acting) Corrective Action Planned: This finding was marked as FOIA Exempt (FOIAE) and as a result, the State Comptroller has determined that the resulting corrective actions are FOIAE under §2.2-3705.2 (9.) of the Code of Virginia. Federal awarding agencies and pass-through entities, please see the Appendix titled "Applicable Management Contacts for Findings and Questioned Costs" to request the corrective action planned from the applicable entity. Estimated Completion Date: 12/31/2024
Upgrade End-of-Life Technology 2023-058 DSS	Responsible Contact Person(s): Kevin Platea, Chief Information Officer Corrective Action Planned: This finding was marked as FOIA Exempt (FOIAE) and as a result, the State Comptroller has determined that the resulting corrective actions are FOIAE under §2.2-3705.2 (9.) of the Code of Virginia. Federal awarding agencies and pass-through entities, please see the Appendix titled "Applicable Management Contacts for Findings and Questioned Costs" to request the corrective action planned from the applicable entity. Estimated Completion Date: 12/31/2024
Continue to Update End-of-Life Technology 2023-059 DMV	Responsible Contact Person(s): Nick Danforth, Chief IT Architect Corrective Action Planned: This finding was marked as FOIA Exempt (FOIAE) and as a result, the State Comptroller has determined that the resulting corrective actions are FOIAE under §2.2-3705.2 (9.) of the Code of Virginia. Federal awarding agencies and pass-through entities, please see the Appendix titled "Applicable Management Contacts for Findings and Questioned Costs" to request the corrective action planned from the applicable entity. Estimated Completion Date: 12/31/2024
Upgrade End-of-Life Technology 2023-060 VDOT	Responsible Contact Person(s): Andrew Green, Information Security Division - Information Security Officer Corrective Action Planned: This finding was marked as FOIA Exempt (FOIAE) and as a result, the State Comptroller has determined that the resulting corrective actions are FOIAE under §2.2-3705.2 (9.) of the Code of Virginia. Federal awarding agencies and pass-through entities, please see the Appendix titled "Applicable Management Contacts for Findings and Questioned Costs" to request the corrective action planned from the applicable entity. Estimated Completion Date: 3/31/2024
Improve Vulnerability Management Process 2023-061 DOE/DAPE	Responsible Contact Person(s): Diane Carnohan, Chief Information Security Officer Corrective Action Planned: This finding was marked as FOIA Exempt (FOIAE) and as a result, the State Comptroller has determined that the resulting corrective actions are FOIAE under §2.2-3705.2 (9.) of the Code of Virginia. Federal awarding agencies and pass-through entities, please see the Appendix titled "Applicable Management Contacts for Findings and Questioned Costs" to request the corrective action planned from the applicable entity. Estimated Completion Date: 6/1/2024
Improve Vulnerability Management 2023-062 VDH	Responsible Contact Person(s): Suresh Soundararajan, Chief Information Officer Othello Dixon, Acting Information Security Officer Corrective Action Planned: ISO met with CIO in November 2023; VDH discussed a plan of action and the next steps. VDH has weekly meetings on Monday with the OIM Technical Point of Contact (POC) to review current vulnerabilities and ensure they are being remediated promptly. Before the meeting, ISO sent the spreadsheet to the POCs to work on their assigned vulnerabilities. VDH began the meeting by reviewing the spreadsheet, action items, and progress on identified vulnerabilities from the previous week. After the meeting, ISO runs a scan to verify that the POC's remediated vulnerabilities are indeed remediated. ISO provides bi-weekly updates to CIO on the vulnerabilities. Implementation Timeline: This is an on-going process. Estimated Completion Date: 6/30/2024
Improve Vulnerability Management Process 2023-063 DBHDS	Responsible Contact Person(s): Glenn Schmitz, Chief Information Security Officer Corrective Action Planned: Currently the vulnerability management program remediation timelines are more aggressive than the VITA guidance. DBHDS will continue to refine and mature the program to meet DBHDS's more aggressive remediation requirements. Estimated Completion Date: 12/31/2024

Audit Finding Reference Number	Responsible Person(s) Corrective Action Planned Estimated Completion Date
Continue to Improve Risk Assessment Process 2023-064 DBHDS	Responsible Contact Person(s): Glenn Schmitz, Chief Information Security Officer Corrective Action Planned: The Risk Assessment Process is built into the BIA process and will be addressed for each application. Due to the current number of applications in the inventory, resource constraints, and competing priorities, this effort will take approximately 3 years to fully complete as part of the standard 3 year BIA certification process. Estimated Completion Date: 12/31/2027
Improve IT Contingency Management Program 2023-065 DBHDS	Responsible Contact Person(s): Glenn Schmitz, Chief Information Security Officer Corrective Action Planned: The Security Office in coordination with the facilities and the faculties' Emergency Coordinator are working together to standardize COOP plans. DBHDS is currently enrolled in the VITA Disaster Recovery (DR) program as well as participates in the annual VITA DR Exercise. Estimated Completion Date: 12/31/2024
Continue Developing Record Retention Requirements and Processes for Electronic Records 2023-066 DSS	Responsible Contact Person(s): Kevin Platea, Chief Information Officer Stephen Schleck, Associate Director of Enterprise Business Solutions Corrective Action Planned: A Change Request for the case management system was developed 2 years ago and DSS is reviewing the change request to determine a status. It was agreed by Line of Business and ITS EBS & a vendor (the systems provider) that there will be an iterative approach to completing the record retention and purge rules for implementation in the case management system. Estimated Completion Date: 12/31/2024
Improve Web Application Security Controls 2023-067 DMV	Responsible Contact Person(s): Beau Hurley, Chief Information Security & Agency Risk Management Corrective Action Planned: This finding was marked as FOIA Exempt (FOIAE) and as a result, the State Comptroller has determined that the resulting corrective actions are FOIAE under §2.2-3705.2 (9.) of the Code of Virginia. Federal awarding agencies and pass-through entities, please see the Appendix titled “Applicable Management Contacts for Findings and Questioned Costs” to request the corrective action planned from the applicable entity. Estimated Completion Date: 12/31/2024
Improve IT Risk Management and Contingency Planning Program 2023-068 DOA	Responsible Contact Person(s): Frank Pitera, Information Security Officer Corrective Action Planned: The agency's ISO is actively working on updating all System Security Plans to conform with the new policy and is targeting June 30, 2024 for completion. Estimated Completion Date: 6/30/2024
Complete a System Security Plan for Each Sensitive System 2023-069 UVAH	Responsible Contact Person(s): Amy Karr, Health System Technology Services Corrective Action Planned: UVA Health has a process in which sensitive applications are reviewed by third party risk assessors on an annual basis. The assessments that are performed review all security controls based on the applications Framework. The software in which this information is collected defines if a control is implemented and, in some cases, how it’s implemented. UVA Health will create individual system security plans for each of these applications based on information collected during these third-party assessments. The system security plans will include information and details on the controls in place or not present. These system security plans will be reviewed by the System Administrators on an annual basis and a process will be developed for notifying HIT Security of any changes to security controls throughout the year. This work is expected to be completed by April 30, 2024. Estimated Completion Date: 4/30/2024
Improve Security Awareness Training Program 2023-070 DBHDS	Responsible Contact Person(s): Glenn Schmitz, Chief Information Security Officer Corrective Action Planned: The security office has begun reviewing training reports on a monthly basis. Any new hire user that has exceeded 30 days of training without completion will have their account disabled until the user's manager can provide justification as to why the user was not able to complete their training. Upon re-enablement, the user will have 30 days to complete. Estimated Completion Date: 12/31/2024
Improve Security Awareness Training 2023-071 VCU	Responsible Contact Person(s): Dan Han, Chief Information Security Officer Corrective Action Planned: VCU is actively revising how mandatory training is being managed and will identify methods to place consequences on individuals who fail to complete the required training. Additionally, VCU will implement a mandatory annual role-based training with associated tracking for its IT staff. Estimated Completion Date: 6/30/2024
Continue to Ensure ITISP Suppliers Meet all Contractual Requirements 2023-072 VITA	Responsible Contact Person(s): Naveen Abraham, Chief Core Infrastructure Services Corrective Action Planned: Ensuring that infrastructure suppliers fulfill all contractual requirements with respect to Commonwealth security policies and standards necessitates a programmatic, continuous improvement approach. VITA has made improved cybersecurity a primary goal and major initiatives have completed and are underway. VITA has established a scoring mechanism, based on the Common Vulnerability Scoring System (CVSS), that delineates the necessary response based on the criticality of the vulnerability (critical, high, and medium). For vulnerabilities with a CVSS score of (critical and high), service level agreement (SLA) 1.1.3 is now in place to measure supplier performance and adjust supplier compensation accordingly through SLA credits and RCDs. For vulnerabilities below the critical and high score, in Q4 of 2023, suppliers started providing data in a quarterly report to the MSI and VITA. The new SLAs combined with the reports of vulnerabilities below the critical and high score are used to ensure suppliers’ contractual compliance. VITA’s data shows that patches for software on the enterprise software list are being applied on an ongoing basis. VITA will work with agencies and suppliers if there are any new technical difficulties or questions about patching. New tools are now available to agencies so that they can monitor and verify the remediation of the vulnerabilities for which infrastructure suppliers are responsible. Dashboards have also been provided to the suppliers so that they can review a shared and common vulnerability list. VITA and the suppliers monitor and review enterprise level logs and security events on behalf of customer agencies through the system dashboard and a 24x7 Security Operations Center. The dashboard is available for access by agencies as of Q4 2023. VITA will continue to monitor and improve the security of infrastructure services through ongoing governance, including the requirements of architecture documentation, system security plans, and audit reports. VITA’s infrastructure services group will work with the VITA security group to confirm that the current state achieves security standards compliance. Estimated Completion Date: 6/30/2024

Audit Finding Reference Number	Responsible Person(s) Corrective Action Planned Estimated Completion Date
Continue to Improve Off-Boarding Procedures 2023-073 DBHDS	Responsible Contact Person(s): Tracy Salisbury, Acting Chief Human Resources Officer Corrective Action Planned: While the standard form created in 2022 was a good tool, facilities were resistant to fully implement it. A workgroup will create a better electronic format that includes all the required processes and meets the needs of the facilities and CO. Estimated Completion Date: 12/31/2024
Improve Controls over the Payroll Certification Process 2023-074 DBHDS	Responsible Contact Person(s): Nathan Miles, Chief Financial Officer Corrective Action Planned: DBHDS will send out an updated checklist regarding all steps associated with payroll certification and reconciliation. These steps will be updated to reflect the October, 2022 implementation of the human capital management system. Also, a small work group of CFOs at the facility level and the Central Office Fiscal Services Director will be formed to develop specific written procedures applicable to all facilities and the Central Office. Estimated Completion Date: 7/1/2024
Continue to Improve Controls over Payroll Reconciliations 2023-075 DBHDS	Responsible Contact Person(s): Nathan Miles, Chief Financial Officer Corrective Action Planned: DBHDS will send out an updated checklist regarding all steps associated with payroll certification and reconciliation. These steps will be updated to reflect the October, 2022 implementation of the human capital management system. Also, a small work group of CFOs at the facility level and the Central Office Fiscal Services Director will be formed to develop specific written procedures applicable to all facilities and the Central Office. Estimated Completion Date: 7/1/2024
Continue to Improve Controls over the Retirement Benefits System Reconciliation 2023-076 DBHDS	Responsible Contact Person(s): Tracy Salisbury, Acting Chief Human Resources Officer Corrective Action Planned: With a benefits SME now on board at CO, DBHDS will have better controls over the HR portion of Retirement Benefits System Reconciliation that will assist facility benefits administrators as needed. Additionally, there will be a session on this topic at the next HR Forum. Estimated Completion Date: 12/31/2024
Improve Internal Controls over Employee Termination Process 2023-077 DOC/CA	Responsible Contact Person(s): Lucinda R. Childs-White, Human Resources Director Corrective Action Planned: Property Collection: 1. The separation checklist is currently being modified for HR staff to confirm/certify Commonwealth property has been collected. 2. The expectations for confirming property collection have been discussed and will be reinforced through future Statewide HR Staff Meetings after the separation checklist modification has been completed. Keying Out Terminated / Separated Employees: (Human Capital Management System) 1. Update Operating Procedure 175.1, Employee Separations, to align with Commonwealth Standards for removal (24 hours), except during established data freezes. 2. These expectations for keying separated/terminated employees have been discussed and will be reinforced through future Statewide HR Staff Meetings. 3. The Office of Human Resources (central office) will conduct periodic reviews to ensure compliance with these expectations. Windows User Accounts: 1. A Human Resource Director Memorandum will be distributed to all Organizational Unit Heads and Human Resource Officers, emphasizing the requirements for the user's supervisor, HRO, or Unit Head to disable the Windows User Accounts within 24 hours of employee separations. 2. Updates to Operating Procedure (OP), Employee Separations and specific OP are in progress to align with the Commonwealth's Security Standards for removal (24 hours). 3. The expectations for timely deactivation of Windows User Accounts have been discussed through a Statewide HR Staff Meeting and will be reinforced after issuance of the statewide memorandum. Estimated Completion Date: 7/1/2024
Improve Internal Controls over Employee Separation Process 2023-078 ABC	Responsible Contact Person(s): John Singleton, Director of Human Resources Corrective Action Planned: The Authority concurs with the exceptions noted and will enhance controls over the employee separation process. The Authority will reassess current processes and ensure all responsible leaders are following the guidelines related to the separation checklist. Furthermore, the Authority will provide additional training and support to the responsible leaders and will conduct quarterly audits to ensure compliance. Estimated Completion Date: 6/30/2024
Improve Internal Controls over Employee Offboarding Process 2023-079 VDH	Responsible Contact Person(s): Twinkle Oliver, Director of Human Resources Corrective Action Planned: 1. OHR will update the required "Separations for Supervisors" training to include updated Staff Separations Checklist. This training is also required for all HR staff. Due date-March 15, 2024 (OHR will escalate notifications to ensure deadline is met.) 2. OHR will create a required "Separations for HR Staff" training outlining responsibility for HR staff. To be completed by June 30, 2024. 3. OHR will increase audits for Staff Separation Checklists for all staff--Classified, Wage & VDH Workers. These audits will include a review to ensure completion of the checklist. To begin by June 1, 2024. 4. OHR will create a Separations Policy that will include information which includes progressive disciplinary action should the policy/process be violated. Estimated Completion Date: 6/30/2024

Audit Finding Reference Number	Responsible Person(s) Corrective Action Planned Estimated Completion Date
Reconcile the Commonwealth's Retirement Benefits System 2023-080 DSS	Responsible Contact Person(s): Melinda Raines, Director of Human Resources Karen Holt, Human Resources Business Process Consultant Corrective Action Planned: DSS is working to improve and update the internal processes of reconciling retirement contributions. Human Resources will review the CAPP Manual Topic 50410 and the Bureau's Scope of Services Manual to have an adequate understanding of the responsibilities in relation to reconciling retirement benefits systems information by October 1, 2023. If needed, DSS will also seek assistance from the Payroll Service Bureau to ensure reconciliations are completed as required. DSS will also review and revise written policies and procedures to reconcile the Commonwealth's retirement benefits system including the monthly reconciliations between the Commonwealth's retirement benefits system and the human capital management system and reviewing cancelled records reports in that system. Estimated Completion Date: 12/31/2024
Improve Processes over Employment Eligibility Verification 2023-081 UVA	Responsible Contact Person(s): Jennifer Weaver, Manager Talent Support Corrective Action Planned: EVP-COO, UVA HR and Provost have implemented multiple changes to meet I-9 compliance requirements, including internal procedures with impact to operations within and between UVA HR and schools/business units. Changes made: (1) UVA HR system: - Help text, notifications, and additional upload document step have been added to the I-9 process in the system for Academic (excluding Wise) employees only; - Steps taken to ensure employee and manager more clearly understand what needs to be submitted and when, including acceptable documentation and guidance on how to provide documentation - I-9 Compliance Dashboard; includes real-time "Incomplete I-9 Report" available to all managers (2) Website changes: additions to Student Hiring Website include updated language to more clearly explain I-9 process and deadlines (3) Communications sent to managers, new hires, those involved in I-9 process (4) Beginning April 17, 2023, a new procedure is in place whereby any student worker who remains non-compliant by 1:00pm on day 4 of employment will be terminated. The student worker and their hiring manager will be notified on days 3 and 4 of this termination. The student may be rehired to their position; however, the hiring manager must start the process from the beginning. Estimated Completion Date: 6/30/2024
Improve Timekeeping Controls 2023-082 UVAH	Responsible Contact Person(s): Douglas E. Lischke, Medical Center Controller's Office Corrective Action Planned: The Medical Center has revised its timekeeping policy to establish expectations for supervisor approval of timecards each pay period. This includes a process to monitor adherence to the policy via an automated system for communication and management reporting. This finding has been resolved. Estimated Completion Date: 9/1/2023
Improve Oversight of Third-Party IT Service Providers 2023-083 VITA	Responsible Contact Person(s): Amy Braden, Director - Security Governance Corrective Action Planned: In general, the security oversight of IT infrastructure services suppliers is working and effective. VITA agrees with the finding; however; that there is a need to mature and improve process and review documentation. VITA plans to investigate whether an earlier delivery or more review time is needed to obtain and review the SOC documentation. VITA's contracts with IT infrastructure suppliers require those providers to submit SOC2 reports annually, and, if a supplier is late in submitting a SOC report, VITA will continue to follow up and, if need be, open a governance case to press for resolution. Where infrastructure suppliers work together with other companies to provide services and VITA contracts directly with such other companies, VITA will continue to independently obtain and review SOC reports from such other companies through those contracts and database oversight processes. By contrast, where infrastructure suppliers use subcontractors with whom VITA does not contract directly, and where the infrastructure suppliers are contractually responsible for the performance of such subcontractors, VITA will exercise oversight and governance over the tower suppliers, aided by the MSI. Estimated Completion Date: 6/30/2024
Develop and Implement a Third-party Service Provider Oversight Process 2023-084 TAX	Responsible Contact Person(s): Andy Hallbert, Information Security Officer Vengatesh Agaram, Chief Information Officer Kristima Brekke, Director of Purchasing Corrective Action Planned: Build out the Supply Chain Risk Management Policy, Standards, and Procedures to comply with recommendation and applicable Commonwealth policies. Estimated Completion Date: 7/31/2024
Obtain, Review, and Document System and Organization Control Reports of Third-Party Service Providers 2023-085 DSS	Responsible Contact Person(s): Kevin Platea, Chief Information Officer Corrective Action Planned: DSS has 15 plus applications that are in active oversight; IT Business Administration is in receipt of the required SOC 2, Type 2 reports. However, additional requirements to capture the SOC 1, Type 2 reports have not yet been accomplished. Several SOC reports were not captured by VITA and then provided to DSS for review. Additional requirements to capture SOC 1, Type 2 reports have been identified and VITA is requesting this information of the providers. Estimated Completion Date: 12/31/2024
Improve Third-Party Oversight Process 2023-086 DMAS	Responsible Contact Person(s): Steve Hanoka, Chief Information Security Officer Corrective Action Planned: This finding was marked as FOIA Exempt (FOIAE) and as a result, the State Comptroller has determined that the resulting corrective actions are FOIAE under §2.2-3705.2 (9.) of the Code of Virginia. Federal awarding agencies and pass-through entities, please see the Appendix titled "Applicable Management Contacts for Findings and Questioned Costs" to request the corrective action planned from the applicable entity. Estimated Completion Date: 4/1/2024
Continue Improving Oversight of Third-Party Service Providers 2023-087 ABC	Responsible Contact Person(s): Diane Enroughty, Information Security Governance Risk & Compliance Manager - Information Security Officer Corrective Action Planned: The Authority will request and review the System and Organizational Controls (SOC) report for high risk, or sensitive systems, on an annual basis and will review the medium risk providers once every three years. ABC will also work with IT Procurement to address the review of contracts to ensure that vendors are required to submit a SOC report. Estimated Completion Date: 6/30/2024

Audit Finding Reference Number	Responsible Person(s) Corrective Action Planned Estimated Completion Date
Continue Improving Service Provider Oversight 2023-088 VDOT	Responsible Contact Person(s): Andrew Green, Information Security Division - Information Security Officer Corrective Action Planned: Document an internal ECOS policy to codify the requirements implemented for previous years. Estimated Completion Date: 9/30/2024
Improve Procedures and Process for Oversight of Third-Party IT Service Providers 2023-089 VAL	Responsible Contact Person(s): Paul Battle, Director of Information Security Corrective Action Planned: Lottery will develop and maintain a complete list of service providers in scope, develop a formal policy, develop and include database terms and conditions in contracts to address the areas identified. Estimated Completion Date: 5/1/2024
Improve IT Service Provider Oversight 2023-090 VCU	Responsible Contact Person(s): Dan Han, Chief Information Security Officer Corrective Action Planned: VCU will adhere to its standards and procedures to ensure the annual review of assurance documentation for its core service providers. The university will also evaluate and determine which subservice providers are significant to the University's operations. The university will attempt to obtain additional third-party attestation or alternative documentation for these sub-service providers, evaluate them if they are made available through the service providers, and document the results of the procedures performed. Estimated Completion Date: 6/30/2024
Improve Third-Party Service Provider Process 2023-091 DOE/DAPE	Responsible Contact Person(s): Diane Carnohan, Chief Information Security Officer Corrective Action Planned: DOE Office of Cybersecurity and Risk Management has completed and implemented policy and procedures. DOE is working with Procurement and Technology for an enhancement to the request portal for applications as well as the workflow in an application to keep track of all tasks associated with DOE 3rd Party vendor applications. Estimated Completion Date: 6/1/2024
Ensure Compliance with the Conflict of Interests Act 2023-092 DBHDS	Responsible Contact Person(s): Tracy Salisbury, Acting Chief Human Resources Officer Corrective Action Planned: Continued focus on the SOEI and required training (every 2 years) has proven to be successful. The oversight of SOEI was transferred to the Deputy HR Director in 2023 -- 100% compliant. Estimated Completion Date: 12/31/2024
Monitor Internal Procedures to Ensure Compliance with the Conflict of Interests Act 2023-093 DSS	Responsible Contact Person(s): Melinda Raines, Director of Human Resources Karen Holt, Human Resources Business Process Consultant Corrective Action Planned: In 2018, the Virginia Department of Social Services (DSS) implemented written procedures to administer the Conflict of Interests Act (COIA) as outlined in the Code of Virginia. While an SOEI policy was not created, the procedures were clear, documented, and administered. DSS continues to refine written procedures and correct identified deficiencies to meet compliance with the COIA. In January 2022, DSS began the process to have oversight responsibility for the COIA reassigned to another Human Resources (HR) unit. HR continues to evaluate and update the approach used to identify and track employees in a position of trust upon hire or change in responsibilities. Prior to the annual disclosure process the SOEI coordinator will review positions against Executive Order 18 (2022) to confirm positions within the agency that are designated as positions of trust. Division directors from various areas will be consulted to determine if any positions involving contracts, licenses, audits, budgets, policy, or grants should be designated in a position of trust. Team members from HR will review the designation list and any additions or removals from the prior year will be updated in the economic interest field in the human capital management system. To capture new hires and transfers in a position of trust throughout the year, the SOEI coordinator will review the new hire and transfer report for the agency twice per month. When a new hire or transfer is moving into a position of trust the employee's information will be added into the Conflict of Interest Disclosure System. Notifications will be sent requesting the disclosure form is completed on or prior to the employee's start date. The system will be monitored to track progress of completion. Should the employee not complete the financial disclosure, the employee's supervisor will be notified. When new employees in a position of trust receive access to the Commonwealth of Virginia Learning Center (COVLC), they are enrolled into the conflict of interest (COI) training and provided a deadline for completing the course. The SOEI coordinator will monitor the COVLC system for completion. Should the employee not complete the orientation training, the employee's supervisor will be notified. To improve monitoring and tracking of COI training every two years, a spreadsheet will be maintained listing training completion dates. The report will be monitored on the same schedule as the new hire and transfer report. The spreadsheet will flag a filer's record when the most recent training date approaches the two year mark and needs to be retaken. HR will then enroll the employee in the COI training, notify the employee and the employee's manager of the training requirement, and monitor for completion. Reassigning oversight of the COIA to another HR unit and following the updated written procedures should show considerable improvement and compliance with the agency's monitoring of the COIA by April 1, 2024. Estimated Completion Date: 4/1/2024
Improve Retirement Benefit Calculations 2023-094 VRS	Responsible Contact Person(s): Robert Irving, Customer Services Director Shanta Harris, Chief Customer Programs Officer Corrective Action Planned: 1) Implement a second approver step for hazardous duty retirements. 2) Implement system data query to identify instances of employer updates to retired or retiring member salaries where there is no "adjustment required" workflow initiated. 3) Implement system code fix to correct the issue of the system not determining the correct life insurance amount due to referencing the month of death in the calculation rather than the month prior to death. Estimated Completion Date: 9/30/2024

Audit Finding Reference Number	Responsible Person(s) Corrective Action Planned Estimated Completion Date
Improve Accounts Payable Controls 2023-095 UVAH	Responsible Contact Person(s): Douglas E. Lischke, Medical Center Controller's Office Corrective Action Planned: Contract Labor: The Medical Center streamlined the approval processes for one contract labor agency for traveling nurses, due to challenges with receiving approvals within the 15 day payment terms, and to ensure no interruption to patient care. The control relied upon was the same control used for employees: management approval of timecards through the Medical Center timekeeping system which the contract labor agency uses to create the invoices. Segregation of Duties: During a critical system go live, the Medical Center placed the Accounts Payable Manager into a dual role over AP and Purchasing to ensure the continuity of patient care. This created a known control risk, that was mitigated via manual processes. Management has led multiple internal and external reviews of these controls, and the findings have been resolved. Estimated Completion Date: 10/1/2023
Perform Complete Physical Inventory 2023-096 UVA/AD	Responsible Contact Person(s): Andrew McGehee, Director of Business Assets and Cost Recovery Corrective Action Planned: UVA migrated over 28,000 assets from one system to another in July 2022. All assets transferred into the new system with financial data fields intact, but the inventory data fields did not migrate cleanly. UVA/AD inventory specialist, along with other temporary workers allocated a tremendous amount of time reviewing and updating the inventory data during FY23. Additionally, the scanners used in UVA/AD inventory process required outside testing and problem solving from UVA/AD inventory management platform company which impacted business processes. Data validation and all integrations were implemented with the team scanning and performing the inventory process, albeit with a backlog due to the overall asset volume. All conversion data and associated sub-system integrations with both the Financial System of record and inventory technology sub-systems scanners are fully operational with inventory specialist starting a full inventory scan to be completed by the end of FY24, prioritizing any equipment outside of the two-year timeframe. UVA has 19,705 in service assets designated as moveable equipment. 6,809 of those assets have an inventory date outside of two years. Of the total outside the two-year mark, 6,024 or 88.5% of those assets have an inventory date within FY21 and 76% have a date in the 3rd or 4th quarter FY21. Estimated Completion Date: 6/30/2024
Perform Responsibilities Outlined in the Agency Monitoring Plan 2023-097 DSS	Responsible Contact Person(s): Ross McDonald, Director of Compliance Ousman Kah, Subrecipient Monitoring Coordinator Corrective Action Planned: A Grants Management solution is being pursued by DSS in anticipation that it can be deployed with Subrecipient Monitoring capabilities needed to comply with these requirements. A new budget request has been submitted for funding of a contingent Subrecipient Monitoring System solution. This will help bridge the deficiencies noted until an integrated permanent solution is implemented. Estimated Completion Date: 3/31/2025
Review Non-Locality Subrecipient Single Audit Reports 2023-098 DSS	Responsible Contact Person(s): Ross McDonald, Director of Compliance Ousman Kah, Subrecipient Monitoring Coordinator Kevin Platea, Chief Information Officer Corrective Action Planned: A Grants Management solution is being pursued by DSS in anticipation that it can be deployed with Subrecipient Monitoring capabilities needed to comply with these requirements. A new budget request has been submitted for funding of a contingent Subrecipient Monitoring System solution. This will help bridge the deficiencies noted until an integrated permanent solution is implemented. Additionally, an interim solution is being considered where these subrecipients will be reviewed and tracked through a manual system. Estimated Completion Date: 3/31/2025
Communicate Responsibilities to Subrecipient Monitoring Coordinators 2023-099 DSS	Responsible Contact Person(s): Ross McDonald, Director of Compliance Ousman Kah, Subrecipient Monitoring Coordinator Corrective Action Planned: The final version of the agency's Monitoring Plan was completed. Estimated Completion Date: 8/1/2023
Evaluate Subrecipients' Risk of Noncompliance in Accordance with Federal Regulations 2023-100 DSS	Responsible Contact Person(s): Diana Clark, Associate Director Senior Corrective Action Planned: A risk assessment tool was developed as part of the State Fiscal Year 2024 SRM Plan and will be implemented with the new plan. Estimated Completion Date: 8/1/2023
Verify that Monitoring Plan Includes All Subrecipient Programmatic Activities 2023-101 DSS	Responsible Contact Person(s): Diana Clark, Associate Director Senior Corrective Action Planned: SRM for the TANF Federal grant program will be included in the SFY2024 SRM Plan. Inclusion of Risk Assessment criteria have been made and are being incorporated into the Monitoring Plan. Estimated Completion Date: 8/1/2023
Confirm Monitoring Activities are Conducted in Accordance with the Monitoring Plan 2023-102 DSS	Responsible Contact Person(s): Diana Clark, Associate Director Senior Corrective Action Planned: A spreadsheet to track monitoring activities by the BP SRM Coordinator was developed and implemented to ensure that Program Consultants adhere to the developed schedule. The BP SRM Coordinator reviews the completed audit documents to ensure that all required audit documents are uploaded to the system timely and that reviews are conducted in accordance with the SRM Plan. A SRM monitoring desk tool will be created for Practice Consultants as a quick reference to the SRM Plan. Training for all Program Consultants conducting SRM will be provided on the new updated monitoring plan as well as ongoing training for newly hired Program Consultants. Estimated Completion Date: 8/1/2023

Audit Finding Reference Number	Responsible Person(s) Corrective Action Planned Estimated Completion Date
Monitor Case Management System Records to Ensure Compliance with TANF Eligibility Requirements 2023-103 DSS	Responsible Contact Person(s): Angela Morse, Director of Benefit Programs Frank Smith, Associate Director Senior Benefit Programs Denise Surber, EAP Manager - Division of Benefit Programs Corrective Action Planned: DSS will work to provide additional training to local agency eligibility workers on how to properly determine and document eligibility determinations in the case management system. Additionally, DSS will consider monitoring local agency eligibility worker's use of manual overrides to confirm that they properly document eligibility determinations in the case management system. Estimated Completion Date: 12/31/2024
Obtain Reasonable Assurance over Contractor Compliance with Program Regulations 2023-104 DSS	Responsible Contact Person(s): Angela Morse, Director of Benefit Programs Frank Smith, Associate Director of Benefit Programs Corrective Action Planned: DSS has requested the vendor's records. Once received, DSS will audit those records to provide reasonable assurance that the contractor administered the LIHWAP federal grant program in accordance with federal statutes, regulations, and the terms and conditions of the federal award before it closes the grant award. Estimated Completion Date: 6/30/2024
Implement Internal Controls over TANF Federal Performance Reporting 2023-105 DSS	Responsible Contact Person(s): Angela Morse, Director of Benefit Programs Mark Golden, Economic Assistance and Employment Manager Division of Benefit Programs Corrective Action Planned: Perform an analysis of identified reporting errors to determine causality and the appropriate actions to resolve reporting errors. Create a systems modification request to correct errors that are identified as occurring as a result of inaccurate programming in the data modification phase of federal report creation. Estimated Completion Date: 6/30/2024
Implement Internal Controls over TANF Federal Special Reporting 2023-106 DSS	Responsible Contact Person(s): Angela Morse, Director of Benefit Programs Frank Smith, Associate Director of Benefit Programs Corrective Action Planned: DSS will perform an analysis of identified reporting errors to determine causality and the appropriate actions to resolve reporting errors. Additionally, DSS will create a systems modification request to correct errors that are identified as occurring as a result of inaccurate programming in the data modification phase of federal report creation. Estimated Completion Date: 12/31/2024
Strengthen Internal Controls over FFATA Reporting 2023-107 DSS	Responsible Contact Person(s): Ida Witherspoon, Chief Financial Officer Corrective Action Planned: Send periodic e-mail reminders to program staff responsible for submitting FFATA data to the Federal Reporting Unit for submission to the federal government. Additional time is needed to fully implement an automated solution. Estimated Completion Date: 10/30/2024
Confirm Subrecipient Suspension or Debarment Status 2023-108 DCJS	Responsible Contact Person(s): Kassandra Bullock, Director of Grants Management DeAndrea Williams, Grants Admin Supervisor Joseph Thompson, Grants Compliance Supervisor John Colligan, Director of Finance and Administration Corrective Action Planned: (1) Staff generate SAM report to check for Exclusion and/or Debarment as well as an active SAM Registration for all federally funded programs and Staff will confirm by checking the Office of the Inspector General's federal Debarment and uploading results to awardee file in On-line Grant Management System (OGMS) to demonstrate proof of status; (2) DCJS OGMS has been updated to ensure all applicants certify to SAM registration status and Exclusion/Debarment Status; (3) Program Staff have been informed to ensure all federal funding opportunities include in the required application materials the "Certification Regarding Lobbying and Debarment"; and (4) Grant Fiscal Monitors confirm the UEI active status of all claims prior to approving disbursements. Estimated Completion Date: 1/26/2024
Ensure Compliance with FFATA Reporting Requirements 2023-109 DCJS	Responsible Contact Person(s): Kassandra Bullock, Director of Grants Management DeAndrea Williams, Grants Admin Supervisor Joseph Thompson, Grants Compliance Supervisor John Colligan, Director of Finance and Administration Corrective Action Planned: An internal compliance review has been implemented to ensure accuracy and timely reporting of FFATA data. Data is confirmed prior to upload by the Grants Compliance Team to address errors, missing information, and conflicting dates. Training has occurred via the Federal Funding Accountability and Transparency Act Subaward Reporting System (FSRS) by Grants Admin staff. Additionally all changes in statements of grant awards (SOGA) will be reviewed and reissued when needed and data re-entered to ensure FFATA correlates with SOGA. Estimated Completion Date: 1/26/2024