



COMMONWEALTH of VIRGINIA

DAVID A. VON MOLL, CPA
COMPTROLLER

Office of the Comptroller

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

March 8, 2018

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, 2017 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) 225-2109.

Sincerely,

David A. Von Moll

David A. Von Moll
State Comptroller of Virginia

COMMONWEALTH OF VIRGINIA
Corrective Action Plan
For the Year Ended June 30, 2017

Fiscal Year	Final Finding No.	Title of Finding	State Agency	Initial Corrective Action	Estimated Completion Date	Responsible Contact Person
2017	2017-001	Design and Implement Sound Internal Controls over Fiscal Activities	DOE/COO	<p>1) Modify established roles in Oracle Financials to prevent General Ledger Supervisors and certain users from recording and authorizing transactions. (COMPLETED 12/2017)</p> <p>2) Perform role mapping of user permissions to modified established roles in Oracle Financials to ensure no users have the ability to record and authorize transactions. (IN PROGRESS)</p> <p>3) Perform periodic reviews of financial transactions in Oracle Financials by user ID to ensure no users are recording and authorizing their own transactions. (COMPLETE 12/2017/CONTINUOUS)</p> <p>4) Continue to perform monthly reviews of user roles in Oracle Financials. (COMPLETE/CONTINUOUS)</p> <p>5) Continue internal controls practice that no user roles or mapped user permissions may be modified without Director's authority, documented through EIM ticketing process. (COMPLETE/CONTINUOUS)</p> <p>6) Restrict access to shared reconciliation support documents/files. Preparers of reconciliation electronic files will have read/write access; all other users including reviewers/approvers will have read only access. Due to electronic accessibility of shared files, file folders cannot be restricted without impeding operations; therefore, files will be password protected for read/write authority and restricted to preparers only. (IN PROGRESS)</p>	6/30/2018	Christine Lopilato, Director of Fiscal Services
2017	2017-002	Improve Support and Review of Financial Recording	DOE/COO	<p>1) Modify Move Request Form (used for reclassification journal entries) to require sufficient documented justification, adequate supporting documentation (including Cardinal reports and Oracle Financials reports as appropriate for reconciling journal entries), and review/approval by the Associate Director and/or Director for all journal entries prior to being entered and posted in the General Ledger. (COMPLETED 11/2017)</p> <p>2) Correcting or reversing journal entries must include as supporting documentation attached to the Move Request Form a copy of the original journal entry and adequate justification for reversal of the original journal entry. (IN PROGRESS)</p> <p>3) "Oracle Only" and "Cardinal Only" journal entries must include justification on the Move Request Form for why the transaction is an Oracle Only or Cardinal Only transaction. (IN PROGRESS)</p> <p>4) Transactions keyed directly to Cardinal must include documented explanation for direct entry to Cardinal for download to Oracle. (IN PROGRESS)</p>	6/30/2018	Christine Lopilato, Director of Fiscal Services
2017	2017-003	Require the Review and Approval of Reconciliations	DOE/COO	<p>For the reader's clarification, this finding pertains to the reconciliation between DOE's internal financial management system (Oracle Financials) and its grants management system (OMEGA) only. This finding does not pertain to reconciliations between Oracle Financials and Cardinal.</p> <p>1) Enhance the weekly OMEGA to Oracle Financials reconciliation process previously developed in FY2017 by integrating the weekly reconciliation process into the monthly reconciliations process. DOE implemented a weekly reconciliation between OMEGA paid claims and Oracle Financials vouchers processed in FY2017. Each weekly reconciliation is performed by the Senior Accounting Analyst, and retained for inclusion with the monthly reconciliation process that is documented as reviewed/approved by the General Ledger Manager with final review/approval documented by the Director and/or Associate Director monthly. The monthly review/approval by Fiscal Services management is part of the monthly reconciliation process prior to certification to DOA. (COMPLETED 7/2017)</p> <p>2) Update reconciliation SOPs to reflect enhanced internal controls processes. (IN PROGRESS)</p>	6/30/2018	Christine Lopilato, Director of Fiscal Services

Fiscal Year	Final Finding No.	Title of Finding	State Agency	Initial Corrective Action	Estimated Completion Date	Responsible Contact Person
2017	2017-004	Improve Internal Controls over Financial Reporting of Service Concession Arrangements	VDOT	The Fiscal Division has added a full-time position assigned to infrastructure capitalization, to include reporting on service concession arrangements. VDOT will develop a more comprehensive process to identify, understand, monitor, disclose, and account for service concession arrangements.	6/30/2018	Richard Holte
2017	2017-005	Improve Internal Controls over Financial Reporting	VDOT	Non-Construction Contract commitments - Fiscal Division will work closely with Administrative Division (ASD) to develop processes in identifying and reporting non-construction contract commitments accurately. To implement this new processes, Fiscal and ASD divisions will be reviewing overall non-construction contracts in Cardinal and validating their accuracy with ASD and determine contract commitments for reporting for FY2018. Leave Liability Report - DOA Cardinal Team has been working to update the Cardinal Leave Liability Report according to the DOA's directive. DOA will review and validate the accuracy of program logic of updated Cardinal leave liability report. After DOA's verification, VDOT will review the accuracy of data for reporting FY2018. VDEM Reimbursements - VDOT has already implemented a corrective action plan for VDEM Reimbursements. Now all reimbursements from VDEM for disaster grants are recorded to revenue instead of as expenditure credits.	6/30/2018	Richard Holte
2017	2017-006	Improve Controls over Financial Reporting	DMV	DMV understands its responsibility to accurately prepare CAFR reports and made improvements this year. DMV also understands that there is still work to be done in particular as it relates to all payable and receivable types. While all funds were collected, accounted for and distributed correctly, DMV acknowledges the CAFR reporting errors that were made and know how to correct those for the next reporting period. DMV needs to be more proactive in its approach to financial reporting. Consequently, the Fiscal Year End work plan provided by the DMV Controller to all divisions to ensure they are aware and up to date on DOA requirements will be changing. DMV is in the process of procuring services to assist with redesigning the financial reporting process with a more thorough internal control environment to ensure that all submissions to DMV Finance are accurate and properly reviewed internally before submission to DOA. This will include training of staff, development of checklists, policies and processes to ensure that all financial reporting is completely both timely and accurately.	9/30/2018	Angela Bartlett - Financial Controller
2017	2017-007	Improve Financial Reporting of Unclaimed Property Activity	TRS	Unclaimed Property will ensure financial templates are completed in accordance with accounting principles generally accepted in the United States of America and a reliable method is utilized to estimate the long-term unclaimed property claims liability.	8/30/2018	Vicki Bridgeman
2017	2017-008	Improve Accounting and Financial Reporting Control Environment of Trust Accounting	TRS	Funding for a senior level accounting position for Trust Accounting was included in the Governor's 2018-2020 budget package submitted to the General Assembly. Treasury will begin developing the Employee Work Profile for this position in early March to include restructuring Trust Accounting work responsibilities with an emphasis on succession planning. The goal is to have the position filled by early June 2018. Additionally, Treasury will evaluate the need for a dedicated resource to research and provide guidance on changes in financial reporting standards.	6/30/2018	Kristin Reiter

Fiscal Year	Final Finding No.	Title of Finding	State Agency	Initial Corrective Action	Estimated Completion Date	Responsible Contact Person
2017	2017-009	Improve Collective Knowledge of Annual Accrual Reporting	DMAS	DMAS will enhance formal policies and procedures that document the accrual process, including workflows, timelines, and resulting reports/documentation. In addition, DMAS will establish a review process to include an analysis of historical projections compared to actual accruals, identify unexpected inconsistencies, sufficiently explain variances and update projection data if needed. (Such policies, procedures and review will be completed prior to the next annual accrual submission, September 30, 2018.) In addition, the Budget Division will institute an internal policy that informs Division staff how to effectively streamline audit responses and insure proper information is communicated with external audit staff. This corrective action will ensure that external audit staff receive complete and accurate information regarding accruals. (An email was sent by Budget Director on December 13, 2017 to all Budget Division staff outlining policy and a copy was saved to the Orientation folder on the Division's shared drive.)	9/30/2018	Lanette Walker, Division Director, Budget Division
2017	2017-010	Submit Required Reports Timely	VEC	VEC worked with the vendor to implement the changes necessary to automate the reports. Functionality has been added to VUIS and the reports are now being submitted timely.	12/31/2017	William Walton, UI Director
2017	2017-011	Improve Internal Controls over Reconciliations	DBHDS	DBHDS Central Office will work to ensure that all facilities reconcile FAACS, FMS and CARDINAL and AVATAR, CARDINAL and FMS; accurately, completely and timely with indication of the preparer and approver of the reconciliation.	6/30/2018	Ken Gunn, DBHDS Director of Budget and Financial Reporting
2017	2017-012	Improve Monitoring over Estimated Accounts Payable	UVAH	In addition to the monthly reconciliation of this account, highlighting the components, an additional vendor query will be run against the accounts payable account to either further substantiate the need for the accrual, or to verify the accrual needs to be reversed.	9/30/2017	Kim Holdren
2017	2017-013	Properly Record Fixed Asset Additions	VAL	The Lottery updated its fixed asset policies and procedures, to include adjustments to depreciation to reflect the most appropriate useful life and start date for depreciation.	7/1/2017	Deborah Courtney
2017	2017-014	Complete Annual Review for the Current Claims Processing System	DMAS	DMAS completed the annual user access review in October 2017 and will emphasize the timing of the review to ensure that DMAS completes user access reviews every 12 months. Managers have become more accustomed to the process and are responding faster. DMAS will develop a schedule for user access reviews to incorporate in its policy and procedures to ensure that the review cycle is in compliance with the Security Standard. The process remains manual, DMAS plans to automate the process within the New Claims Processing System. DMAS also intends to improve the process with the implementation of a risk management software and with VITA's Active Directory migration.	6/30/2018	Mukundan Srinivasan, DMAS Chief Information Security Officer, Information Management Division Bill Burnette, DMAS Acting Information Security Officer, Office of Compliance and Security
2017	2017-015	Develop Processes to Facilitate the Controlling of Privileges in the Claims Processing System	DMAS	DMAS will continue to perform the manual access reviews of its Current Claims Processing System and will review for conflicts of segregation of duties and ensure that users have the proper role needed for their responsibilities. The replacement for the Current Claims Processing System (i.e. the New Claims Processing System) will emphasize profile and role-based security. All profiles and roles will be documented in business terms, including a conflict matrix, so that managers, security and IT can clearly see what is being granted and what cannot be granted in combinations. Profiles and role base security will be implemented as each New Claims Processing System module is implemented. All New Claims Processing System components are expected to be implemented by March 31, 2020.	3/31/2020	Mukundan Srinivasan, DMAS Chief Information Security Officer, Information Management Division Bill Burnette, DMAS Acting Information Security Officer, Office of Compliance and Security
2017	2017-016	Remove Access to the Current Claims Processing System in a Timely Manner	DMAS	Currently, the process for removing an individual's Current Claims Processing System access is a completely manual process. DMAS is in the process of developing an automated workflow process for termination of system access. Termination notices will be communicated directly to the Office of Compliance and Security (OCS) by the employee's manager. OCS will have a daily dashboard of employees to be removed from the system. OCS projects this process will be implemented by March 1, 2018.	3/1/2018	Mukundan Srinivasan, DMAS Chief Information Security Officer, Information Management Division; Bill Burnette, DMAS Acting Information Security Officer, Office of Compliance and Security

Fiscal Year	Final Finding No.	Title of Finding	State Agency	Initial Corrective Action	Estimated Completion Date	Responsible Contact Person
2017	2017-017	Ensure Employees have Proper Access Roles within the Commonwealth's Procurement System	DMAS	In September 2017, the account with the 'No Supervisor' role in Commonwealth's procurement system was reassigned from the acting Procurement Manager to the current Procurement and Contract Management (PCM) Division Director. The PCM Division Director or his designee will work as the "Entity Lead" with the System Security Officer and DGS to ensure that proper user access is established and maintained in Commonwealth's procurement system. The Entity Lead will disseminate changes in access roles to the System Security Officer. The System Security Officer will document a standard procedure of administering and reviewing user access and will work with the Entity Lead during the annual user access review. The former DMAS ISO retired during the audit. The acting ISO will obtain Commonwealth procurement system training in order to understand and implement procurement system security requirements for DMAS. This will allow the acting ISO to introduce effective review and revision procedures. The training will be scheduled during the first quarter of 2018 and DMAS OCS will begin directly administering the procurement system by March 31, 2018.	3/31/2018	Mukundan Srinivasan, DMAS Chief Information Security Officer, Information Management Division Bill Burnette, DMAS Acting Information Security Officer, Office of Compliance and Security
2017	2017-018	Strengthen Access Controls	TAX	TAX will initiate a project that documents combinations of access functions that create potential segregation of duties violations. From the documentation, TAX personnel will determine if the potential segregation of duties violation should be controlled via an application access security rule or some other compensating control.	12/31/2018	Kevin Cronin
2017	2017-019	Improve Service Account Management	TAX	TAX will document all service accounts in the system security plans by September 30, 2018. In addition, TAX will implement a tool to facilitate the management of service accounts by April 30, 2019.	4/30/2019	Grayson Walters
2017	2017-020	Address Uncorrelated Accounts	TAX	TAX will correlate each account in the access management system with a unique identity and establish a continuing process to ensure the correlation of all accounts by July 31, 2019.	7/31/2019	Kevin Cronin
2017	2017-021	Improve Documentation over Financial Reporting System Security Functions and Features	TAX	TAX will more fully document policies and procedures related to the security functions and features of TAX's financial accounting and reporting system (Advantage Revenue) by September 30, 2018.	9/30/2018	Vengatesh Agaram
2017	2017-022	Perform Annual Access Review	TAX	This corrective action has two key milestones. By December 31, 2018, TAX will complete an access review for all technology resources currently controlled via its Identity Management System. By December 31, 2020, TAX will complete a project so that all technology resources are managed by its Identity Management System.	12/31/2020	Kevin Cronin
2017	2017-023	Establish and Implement Policies and Procedures for Accessing Budgetary Information	DOE/COO	The Budget Office will develop and implement written policies and procedures for managing access to local shared drives used for establishing state funding amounts for local school divisions. Due to a lack of direct access to VITA reports that show access to DOE's shared drive, the only method currently in place for DOE to access data related to shared drive access is to request the report from VITA. The new policies and procedures will require submission of a request to DOE's Chief Information Security Officer to make a written request to VITA to generate shared drive access reports for periodic monitoring.	6/30/2018	Ed Lanza, Director of Budget
2017	2017-024	Improve Timely Removal of Critical Access	VDH	The VDH Process Improvement Analyst formed a team to review the HR14 process, and multiple solutions are under review by the process improvement team and Deputy Leadership Team. The chosen solution will be utilized to address the recommendation and mitigate as much human error and intervention as possible for terminating user access.	6/30/2018	Becky Bynum, HR Director

Fiscal Year	Final Finding No.	Title of Finding	State Agency	Initial Corrective Action	Estimated Completion Date	Responsible Contact Person
2017	2017-025	Improve Controls for Granting and Restricting Elevated Workstation Privileges	UVA/AD	UVA will assess the risk, implementation timing, approach, and compensating controls in place for workstations that have elevated access or access sensitive data and update policies and standards as appropriate. Considerations will be given to the recommendations of: (1) a formal authorization process, (2) limited access to administrative rights to users who have a documented job related functions that requires the elevated privileges, (3) a documented record of end-users with elevated workstation privileges, (4) an end-user agreement for users with elevated privileges, and (5) additional security training that communicates the associated end user responsibilities and the University's expectations. UVA, through the SecureUVA, is implementing end-point detection tools that will enable visibility, prevention, detection and response to workstations that are used by individuals that have access to the highest risk data. Tools that are being considered are leading tools in the security industry and the project has been kicked-off. These tools will be implemented on workstations that have elevated privileges or access highly sensitive data. In addition, UVA is implementing a managed workstation solution for users with elevated and privilege access to University systems and those workstations will have these controls.	10/31/2017	Teresa Wimmer, Assistant Vice President for Enterprise Applications David Strite, Assistant Vice President for User Experience & Engagement
2017	2017-026	Improve Information System Access Controls	TRS	Treasury will improve its policies and procedures for assigning access to two of its information systems related to Unclaimed Property to address the findings.	6/30/2018	Vicki Bridgeman
2017	2017-027	Perform Annual Access Certifications for Information Systems	DOC	During the months of January through March of each year the TMS Inventory Management System Coordinator shall perform a review of active TMS user accounts to ensure the TMS access is reasonable based on the employee's current job duties and ensure the level of access is still necessary. This review will be completed and TMS system access adjusted by March 31st of each year.	3/31/2018	Steve McClung - DOC Building and Grounds Director

Fiscal Year	Final Finding No.	Title of Finding	State Agency	Initial Corrective Action	Estimated Completion Date	Responsible Contact Person
2017	2017-028	Perform the Required Information Technology Review	DMAS	<p>DMAS concurs that the Agency did not conduct a security audit of the Current Claims Processing System in the two-year cycle as required pursuant to 45 CFR §95.621. The delay in the biennial audit was due to the U. S. Department of Health and Human Services - Office of Inspector General (OIG) conducting a comprehensive security audit of the Current Claims Processing System that started in September 2015. The OIG auditors used 45 CFR §95.621 – Automated Data Processing System Security Requirements and Review Process as criteria for the audit. In the OIG fieldwork exit conference presentation was held on April 28, 2016. DMAS received the final audit report from the OIG on April 25, 2017. DMAS and the Service Provider have been working to address the audit issues and system vulnerabilities noted in the audit. Due to strained resources for both the Service Provider and DMAS in responding to the audit requests and resolving the audit issues, DMAS chooses not to begin another similar security audit while the OIG was still performing its audit fieldwork and testing. In arriving at this decision, consideration was given to preventing duplication of effort for limited resources. Additionally, the results of the OIG audit provide helpful insight to efficiently develop the scope of the DMAS security audit of the Current Claims Processing System. DMAS worked with Computer Aid, Inc. (CAI) through the COV IT Contingent Labor Contract (Statement of Work Process) to obtain IT services (Security Audits) from a CAI subcontractor. DMAS provide the Statement of Requirements to CAI on September 15, 2016. After reviewing the SOW submitted by the CAI subcontractor, DMAS selected the subcontractor and began negotiating the Statement of Requirements which delayed the start of the audit. The contract between CAI and DMAS was executed on January 23, 2017. The Current System IT Security Audit fieldwork, testing, documentation, and report preparation began after the entrance conference on March 22, 2017 and was completed in October 2017.</p> <p>The results of the OIG Current Claims Processing System Security Audit and the CAI Subcontractor Current Claims Processing System IT security audit will assist DMAS in monitoring the Service Provider to ensure compliance with the Commonwealth Security Standard, CAPP Manual, Code of Federal Regulation, and the contract with the Commonwealth. If any weaknesses are identified in the audits, DMAS will implement complementary controls to mitigate the risk to the Commonwealth until the Service Provider corrects the deficiency. The following milestones for the Current Claims Processing System IT Security Audit project completed the corrective action: 1) The CAI subcontractor issued its draft Current Claims Processing System IT Audit Report on October 18, 2017; 2) DMAS provided responses to the findings on November 17, 2017. Responses were reviewed by Internal Audit and provided to the CAI subcontractor for incorporation into the final report; 3) The CAI subcontractor provided the final audit report to Internal Audit on November 30, 2017 for review; and 4) Internal Audit distributed the final audit report to DMAS management on December 8, 2017 and discussed with the DMAS Director on December 14, 2017. Corrective Action Plans for the recommendations were added to our quarterly tracking of CAP status updates beginning in CY 2018.</p>	12/14/2017	Paul Kirtz, DMAS Internal Audit Director, Internal Audit Division Mukundan Srinivasan, DMAS Chief Information Security Officer, Information Management Division Bill Burnette, DMAS Acting Information Security Officer, Office of Compliance and Security
2017	2017-029	Improve Database Security	TRS	Treasury will develop procedures to ensure the appropriate security control is in place and functioning effectively.	6/30/2018	Deborah Edwards
2017	2017-030	Improve Database Security	DOE/COO	Vendor unable to meet scheduled timelines to upgrade server environment resulting in IT security deficiencies. Multiple concerns will be addressed during the implementation and testing phases of the server upgrade.	12/31/2018	Brian Gibbs-Wilson, Chief Information Security Officer
2017	2017-031	Improve Database Security for Financial Reporting System	DSS	Finding 2017-031 was marked as FOIAE under §2.2-3705.2 of the Code of Virginia due to its sensitivity and description of security controls. Corrective action updates will be provided to the Auditor of Public Accounts under separate cover.	6/30/2018	Barry Davis/Robert Hobbelman
2017	2017-032	Continue Improving Database Security for Case Management System	DSS	Finding 2017-032 was marked as FOIAE under §2.2-3705.2 of the Code of Virginia due to its sensitivity and description of security controls. Corrective action updates will be provided to the Auditor of Public Accounts under separate cover.	6/30/2018	Barry Davis/Robert Hobbelman

Fiscal Year	Final Finding No.	Title of Finding	State Agency	Initial Corrective Action	Estimated Completion Date	Responsible Contact Person
2017	2017-033	Improve Web Application Security Controls	DHRM	Hiring of an IT Data Security staff on July 1, 2018. Gather documentation, perform analysis, develop and implement a solution to resolve finding.	12/31/2018	Belchior Mira
2017	2017-034	Improve IT Risk Management and Disaster Recovery Planning	DHRM	Documenting evaluation of data stored in mission essential/sensitive systems (including regulatory requirements to which the data is subject) as well as potential damages to the agency and Commonwealth if the confidentiality, integrity or availability of this data is compromised.	7/1/2018	Belchior Mira
2017	2017-035	Improve Database and Application Security	DHRM	Hiring of an IT Data Security staff on July 1, 2018. Gather documentation, perform analysis, develop and implement a solution to resolve finding.	12/31/2018	Belchior Mira
2017	2017-036	Improve Application and Database Controls over the Enterprise Resource Planning System	VAL	The Lottery continues to improve application and database controls over the enterprise resource planning system, including the implementation of enhanced monitoring and logging tools in February 2018.	3/31/2018	Ted Maxwell
2017	2017-037	Improve Vulnerability Mitigation Efforts	VAL	The Lottery is modifying its vulnerability and patch management processes by modifying its Vulnerability Scanning Standard to correspond with the Commonwealth's Information Security Standard SEC501.	12/1/2017	Elizabeth Smith
2017	2017-038	Risk Management and Contingency Planning Documentation	VEC	VEC will review and update Risk Management and Contingency Planning documents to ensure SEC501 requirements are met and ensure the information is consistent within each document and reflects the current environment. These documents include: BIA, IT System and Data Sensitivity Classifications, Risk Assessments, Continuity Plan and DRP.	12/31/2019	David Clark, ISO
2017	2017-039	Continue to Improve Database Security	VEC	VEC is in the process of migrating one of our database environments from Virtual to Physical servers. When this is complete, the version of the database will be upgraded and database logging will be enabled.	6/30/2018	Dave Portner, Information Technology Director
2017	2017-040	Improve IT Risk Management Process and Documentation	UVAH	UVAH is in the process of reviewing the current BIA and have plans to complete by June 30, 2018. UVAMC will conduct a risk assessment to include PS financials and the additional functionality added during the EPIC Phase II go-live, to be completed June 30, 2018.	6/30/2018	Erin Trost
2017	2017-041	Improve Database Security	UVAH	UVAH is working with the vendor to correct the identified weaknesses.	6/30/2018	Erin Trost
2017	2017-042	Improve Database Security	ABC	ABC recently upgraded our primary databases to the most current version; after the upgrade, ABC requested that the APA review the databases to ensure that VEC had the proper hardening and controls implemented. The APA provided a list of potential deficiencies and benchmark standards. ABC has implemented the controls and configurations that VEC was able to, and for any that may remain, ABC will document the business need, will explore mitigating, compensating controls, and will pursue security exceptions as may be necessary.	6/30/2018	John Pearson
2017	2017-043	Improve Database Security	DOA	Implemented Auditing DML actions by DBAs/enhanced reporting to include a comprehensive list of audit items.	2/4/2018	Joseph Agabin / Sanjay Garg
2017	2017-044	Improve Database Security	DMV	DMV agrees with the APA on the importance of proper database security supporting mission critical systems and has developed baseline security configurations that exceed the requirements of Commonwealth security standards to meet DMV's needs. As identified during the audit, compliance must be maintained during upgrades and new developments, and oversight on these controls must be performed. To mitigate this finding DMV will strengthen its database maintenance procedures and expand our monitoring capability of the database environment.	9/30/2018	Beau Hurley - Chief IT Security & Agency Risk Management
2017	2017-045	Improve Database Security	VDH	The controls discussed in the communication marked FOIA Exempt have been evaluated, and were either implemented or under further testing to ensure operations are not impacted by implementing the control settings.	6/30/2018	Debbie Condrey, Chief Information Officer

Fiscal Year	Final Finding No.	Title of Finding	State Agency	Initial Corrective Action	Estimated Completion Date	Responsible Contact Person
2017	2017-046	Review and Document Service Organization Control Reports of Third-Party Service Providers	DMAS	Developed new guidelines and procedures in the IT procurement process: a) Listing all required standards in RFP Template including SOC Reports and where to find detail; b) Requiring SOC 2 Type 2 reports in contract requirements for the New Claims Processing System contracts; and c) Establishing reporting timelines for oversight activities when the system is live (SOC II, Type 2 – Initial report due within 90 days of contract effective date, thereafter due annually); and completed following actions for SOC report reviews: a) Developed a SOC report review questionnaire template; b) Used the template to review SOC reports received from the Current Claims Processing System IT Contractor for its IT data center subcontractors; and c) Developed a SOC2 PowerPoint training explaining the SOC2 report, defining its purpose and how to review the document. Corrective Actions to be completed: Develop internal protocol with stakeholders, including PCM, Information Management, Contract Administrators and others as needed, to implement SOC receipt and review requirement for required DMAS contracts. Policies and Procedures to include: 1) Coordination and responsibilities between, PCM, Contract Administrator and subject matter experts; 2) Language in contracts identified as having significant fiscal transactions through use of developed tool for the Contractor to provide appropriate SOC report on a regular basis; Update semi-annual contractor performance evaluation form used by Contract Administrators to include as appropriate: a) Confirmation of receipt of annual SOC report (yearly) from contractor and b) Confirmation of receipt of any Corrective Action Plan; and 4) Include provisions for a DMAS mitigation plan for significant weaknesses found in SOC reports.	9/30/2018	Mukundan Srinivasan, DMAS Chief Information Security Officer, Information Management Division Bill Burnette, DMAS Acting Information Security Officer, Office of Compliance and Security Chris Foca, Division Director, Procurement and Contract Management
2017	2017-047	Improve Oversight of Third Party Service Providers	UVAH	UVAH has developed a comprehensive risk management/assessment framework that applies to third-party vendors. The risk assessment process is a collaborative endeavor involving UVAMC IT Security, Procurement, Clinical Engineering, and Senior Leadership. For third-party vendors, one of the following risk assessments need to be completed: Cloud Risk Assessment, Black Box Risk Assessment, Medical Device Risk Assessment, and Security/Exhibit, Requirements. In addition, UVAH created an annual review process for Iron Mountain, as well as a process to review risk assessments when a contract is up for renewal.	6/30/2018	Erin Trost
2017	2017-048	Increase Oversight over Third-Party Providers	DBHDS	The Department's Information Security (IS) team will create an accurate (ongoing) list of all third party IT service providers to DBHDS. For each relevant Third Party, the appropriate control reports they are obligated to provide by state/federal statute (and by way of established contracts with the Department and/or Commonwealth) will be determined. The IS team (through the Chief Information Security Officer) will, for each relevant third party, make a recommendation to the Chief Information Officer and as to which report(s) will be most informative and helpful in determining proper security/data controls are in place. The Chief Information Officer will review the recommendations, make adjustments and give final approval. Once approved, a process will be established within the IS team (through the Chief Information Security Officer) to review and report on the appropriate reports (per relevant Third Party) within 60 days of publication (with "publication" meaning available to the Department). Each report will contain a security/data safety assessment as well as any recommended actions for the Department to pursue. The Chief Information Officer will review these reports and inform the DBHDS Executive Team of issues and recommended next steps (if any).	7/1/2018	Greg Bell, CISO
2017	2017-049	Continue to Improve Oversight over Third-Party Service Providers	VEC	VEC will continue efforts of maintaining oversight of its third-party service providers. Including identifying outsourced services and providers, ensuring security and reporting requirements are included in contracts, reviewing and evaluating SOC reports, and where applicable, maintaining oversight over ECOS services to confirm that VITA and Providers are compliant with the Security Standard and written agreements. One Exception will be filed with VITA concerning GeoSolutions, which will finalize ECOS with GeoSolutions.	12/31/2019	David Clark, ISO

Fiscal Year	Final Finding No.	Title of Finding	State Agency	Initial Corrective Action	Estimated Completion Date	Responsible Contact Person
2017	2017-050	Continue Improving Oversight of Third-Party Service Providers	DSS	On August 5, 2017, DSS updated Section H- EXTERNAL INFORMATION SYSTEM SERVICES & THIRD PARTY SERVICES (SA-9) of the DSS Information System and Services Acquisition Security Policy. The policy requires the agency to collect and review: SEC 525 GAP Analysis (similar to ECOS checklist); SOC II, Type II audits, or evidence of any IT security audits that were performed to SEC 520 standards against SEC 525 compliance. On a weekly basis Information Security Risk Management (ISRM) is working the department's Division of General Services' Contracting team to review ECOS and non-ECOS documentation. ISRM is on track to document this procedure and attach it to the policy document by the implementation date.	6/30/2018	Barry Davis/Robert Hobbelman
2017	2017-051	Implement Newly Developed Policies over Information Technology Third-Party Service Providers	VCU	VCU has requested assessment and attestation documentation from the identified vendors and has received and completed documentation reviews for over 30% of the identified vendors. VCU expects to complete all annual reviews for identified vendors by June 30, 2018 and further refine the process for upcoming years.	6/30/2018	Dan Han, VCU Information Security Officer
2017	2017-052	Evaluate, Revise, and Implement the Change Management Process	VEC	VEC will update the Change and Configuration Management Plan and processes to address the weaknesses identified.	6/30/2018	Dave Portner, Information Technology Director
2017	2017-053	Develop Baseline Configurations for Information Systems	DBHDS	In consultation with the Agency IT Advisory Committee (AITAC), the Department's Business Solutions Development (BSD) and Production Support (PS) teams will draft an outline categorization of the applicable hardware/software standards and types of testing that need detailing. The BSD and PS teams will then draft, based upon CO knowledge and experience, the details for each category and (when complete) that draft material will be reviewed and adjusted by the AITAC membership. After the AITAC review/modifications, the materials will be presented to the Chief Information Officer for approval and appropriate publication within the Department. The CO development and production support staff has developed a process for documenting the baseline configurations of hardware systems. Baseline standards for software development and testing procedures have been developed and distributed for use by the CO and facilities IT staff. These include the requirement to have separate operational, development and testing environments for software. Specific security configurations for sensitive systems are being developed but have not been propagated. Results from vulnerability scanning will be incorporated into change requests for identified systems.	3/31/2018	Chris Sarandos - DBHDS CIO
2017	2017-054	Improve Information Technology Change Management Program	DMV	DMV recognizes its obligation for the protection of configuration information found within change management requests and is taking the steps necessary to improve it. The current process utilized VITA services that were considered secure in the past but have since been determined deficient for DMV's needs. The agency had multiple representatives on the selection team for the new VITA Managed Service Integrator, and provided security requirements for the change management platform being delivered. With the impending implementation of the new platform this year, DMV feels it's in the best interest of the taxpayers that DMV not invest in new solution today but instead establish a series of mitigating controls that will ensure the required level of protection while DMV focuses agency resources on the migration to the new platform being provided.	10/31/2018	Beau Hurley - Chief IT Security & Agency Risk Management
2017	2017-055	Retain Evidence of Approval for Changes in Local Funding	DOE/COO	The Budget Office currently has a guidance document related to the rebenchmarking process. The final instruction after each step requires a change control form to be written. The document will be revised to ensure that the forms are signed. The rebenchmarking document will be modified to include a step to secure approval signatures for the change control forms as one of its final actions. The Budget Director has also met with budget development staff to remind them of the importance of the change control forms as well as the signatures that accompany them.	6/30/2018	Ed Lanza, Director of Budget
2017	2017-056	Improve Vulnerability Identification and Mitigation Process	DHRM	Hiring of an IT Data Security staff on July 1, 2018. Gather documentation, perform analysis, develop and implement a solution to resolve finding.	12/31/2018	Belchior Mira

Fiscal Year	Final Finding No.	Title of Finding	State Agency	Initial Corrective Action	Estimated Completion Date	Responsible Contact Person
2017	2017-057	Improve Risk Management and Continuity Planning Documentation	VCU	VCU is currently working on further integrating both systems so that system and risk assessment information can be better tracked and organized, allowing this information to be maintained more consistently and accessed in an even faster and more streamlined fashion. VCU recognizes the need to strengthen its business continuity planning and has recently purchased a business continuity software tool to help identify enterprise level risk, conduct BIAs, identify recovery strategies and support overall business continuity programming. This process will be on-going through 2018 with a full University BIA available by the end of the calendar year.	12/31/2018	Dan Han, VCU Information Security Officer
2017	2017-058	Continue to Improve Oversight over IT Risk Assessments	VEC	The agency has made significant progress in documenting Risk Assessments. VEC recently re-evaluated its sensitive systems and identified a total of 27 sensitive systems. An IT Risk Assessment Plan was submitted to VITA outlining the plan for completing these Risk Assessments over the required 3-year period. By the end of June 2018, VEC will have completed 11 Risk Assessments. If funds permit, during the remainder of 2018, VEC plans to complete 8 Risk Assessments, 10 in 2019, and 8 in 2020. Additionally, for Risk Assessments that have been completed, VEC will review and update the Assessment annually.	12/31/2019	David Clark, ISO
2017	2017-059	Upgrade or Decommission End-of-Life Operating Servers	ABC	The server op systems upgrade was dependent upon first upgrading the applications residing on those servers. ABC upgraded the applications and the server operating systems.	9/30/2017	Paul Williams, CIO
2017	2017-060	Continue to Upgrade Unsupported Technology	DBHDS	DBHDS continues to make adjustments to its IT governance structure in an effort to achieve modernization and improved security and service levels -- reference implementation of the Agency IT Advisory Committee (AITAC), November 2015, and the Change Management forum, December 2015, discussed in our response to Management Comment #18. As of December 2015, DBHDS has identified 437 applications, largely because of a previous deficit in Enterprise IT collaboration. By June 30, 2016, the office of the Chief Information Officer will publish an Application Modernization Plan (developed in collaboration with the AITAC membership) that will reduce the number of applications from the current level of 437 to 215 by December 31, 2017. The plan will provide reduction milestones for December 31, 2016, June 30, 2017, and December 31, 2017. DBHDS continues to make improvements in identifying and remediating systems that are utilizing end-of-life technologies. Remediation tools have been acquired and a plan for retirement or remediation of end-of-life systems to a common supported technology will be completed by June 30. Efforts include work being addressed in current projects in the central office such as the ACES project and work being completed at the facilities. The date of December 2017 is obtainable for completion of this finding.	3/31/2018	Greg Bell - DBHDS CISO Chris Sarandos - DBHDS CIO
2017	2017-061	Continue to Upgrade Unsupported Technology	VEC	All systems currently using unsupported technology are targeted to be upgraded or decommissioned by March 31, 2018.	3/31/2018	Dave Portner, Information Technology Director

Fiscal Year	Final Finding No.	Title of Finding	State Agency	Initial Corrective Action	Estimated Completion Date	Responsible Contact Person
2017	2017-062	Continue to Improve Information Security Program and IT Governance	DOE/COO	<p>Information Security Program</p> <ul style="list-style-type: none"> - Develop IT security policies and procedures manual - Track all key Information Security Milestones - Explore resource augmentation <p>IT Systems Hardening and Change Management Process</p> <ul style="list-style-type: none"> - Document baseline configurations to align with the Commonwealth Security Standard and Industry Best Practices - Develop/Update IT System Hardening and database security policies and procedures - Implement a database auditing mechanism - Implement industry benchmarks <p>Risk Management Process</p> <ul style="list-style-type: none"> - Engage vendor to perform Risk Assessments - Develop Risk Assessment policies and procedures - Explore resource augmentation <p>Security Awareness Training</p> <ul style="list-style-type: none"> - Transition from to new Security Awareness Training delivery mechanism - Transition monitoring of completion of IT security awareness training from HR to IS - Develop Information Security Training policies and procedures - Acquire requisite knowledge regarding role based access to IT Security Awareness training - Explore resource augmentation - Consult with other Executive Branch agencies <p>IT Security Audits</p> <ul style="list-style-type: none"> - Engage vendor to perform Sensitive System Audits - Ensure that audits are performed in accordance with Commonwealth IT auditing standards - Continue to pursue funding for audit-compliance systems <p>Submit required Audit Plans to VITA</p> <ul style="list-style-type: none"> - Coordinate with Vendor for firm scheduling dates - Explore resource augmentation 	12/31/2018	Brian Gibbs-Wilson, Chief Information Security Officer
2017	2017-063	Continue to Improve IT Governance	DBHDS	<p>The funding request to remediate the audit finding (Audit Remediation Decision Package) was rejected and final corrective action plans are dependent on funding. DBHDS will review options available when the final budget is approved. Previously the Department instituted the FAIR Project with a strategy to engage an executive-level decision team. The decision team would provide guidance in selecting a core suite of common applications that will be supported by the Central Office, then migrate all facility users to that suite. The remaining facility-specific applications will be modernized and migrated to the agency-wide infrastructure environment at VITA, then all agency applications will be transitioned to a cloud hosting provider using the VITA server hosting multi-supplier model. The net result will be a significant reduction in the number of duplicate applications, a decrease in the cost to support and secure the applications, and a subsequent increase in the quality of application support and function provided to the agency's business units. It is expected that the reduction in DBHDS sensitive IT systems will continue.</p>	6/30/2018	Greg Bell - DBHDS CISO Chris Sarandos - DBHDS CIO
2017	2017-064	Improve Policies, Procedures, and Plans for Backup and Restoration	DSS	<p>DSS is currently developing the Continuity Plan for 2018, due on April 1, 2018. In April, following the Continuity Plan submission, the Continuity Coordinator will meet with all system owners that have a RPO/RTO misalignment with DIS Disaster Recovery and either modify the RPO/RTO, or get a signed acknowledgement that the owner accepts the difference.</p>	6/30/2018	Barry Davis/Robert Hobbelman

Fiscal Year	Final Finding No.	Title of Finding	State Agency	Initial Corrective Action	Estimated Completion Date	Responsible Contact Person
2017	2017-065	Improve IT Contingency Management Program	DBHDS	DBHDS has started an IT COOP / DRP project with a projected completion date of October 1, 2018. This project will develop procedures, assign roles and responsibilities, and update the IT COOPs and DRPs ensuring they are consistent across the agency. DBHDS will ensure these IT COOPs and DRPs are tested annually.	10/1/2018	Greg Bell - DBHDS CISO Chris Sarandos - DBHDS CIO
2017	2017-066	Improve Security Awareness and Training	DHRM	Implementing online classes in the COVLC to provide role based security training to staff with role-based assignments	7/1/2018	Belchior Mira
2017	2017-067	Improve Security Awareness Training Program	UVA/AD	UVA will: a) Update existing policies to address periodic security training and ensure that additional role-based training is included and b) Implement a process to monitor completions and enforce compliance. As part of the SecureUVA program (formerly named the Security Enhancement Program), UVA will update all IT security policies, standards, and guidelines. The requirement for security training, as well as more periodic training updates, will be covered in these updated standards. This project has started and will be completed by June 30, 2017. UVA will also develop methods to track and enforce compliance as part of a second SecureUVA project. This project will be scoped to update the current training materials and training system, which will help track and enforce training requirements.	1/5/2018	Virginia H. Evans, Chief Information Officer Jason C. Belford, Chief Information Security Officer
2017	2017-068	Continue Improving Application Security Controls	DMV	DMV understands the need for a comprehensive set of controls for ensuring proper authentication of applications and is taking the necessary steps to bring DMV's current technical controls into alignment with Commonwealth security standards. For a successful implementation, the underlying infrastructure was first upgraded to ensure a solid platform to build upon. With the new infrastructure in place the development team's effort has been applied to the changes needed in the application to update the controls. Understanding that the impact to the Commonwealth is significant, an extensive amount of code review and testing is required which was the driving force behind the established timeline for the project.	9/30/2018	Beau Hurley - Chief IT Security & Agency Risk Management
2017	2017-069	Improve Policies and Procedures for Removal of Terminated Employee Badge Access	UVAH	Implement new policy, termination of team member badges, that upon notification from Medical Center computing, the ID Badge office has 24 hours to terminate the badge in the system. In addition, to electronically document the termination date of the employee's badge, the date will be entered into the Expiration field in the ID badge system.	9/30/2017	David Cornelius
2017	2017-070	Improve Terminated Employee Procedures	UVA/AD	The current employee off-boarding process is a paper-based, manual process, dependent on hiring unit implementation, collection of signatures, and limited technology. The University is in the process of implementing a new HR Management System for future state employee transaction management and engagement. Additional refinement of off-boarding procedures, inclusive of timeframes for completion, and impacted employee populations, are planned as part of this project. The off-boarding process will be significantly enhanced as an element of the new HR Management System's process capacity, resulting in improvement in compliance with University off boarding procedures. Until the new HR Management System and off-boarding process can be implemented, Human Resources and Provost Office will revisit terminated employee procedures and define a specific timeframe for completing the off-boarding checklist, as well as identify all employee types requiring an off-boarding checklist. The revised procedures will be clearly communicated to all departments. In addition, the University will continue to perform random audits to evaluate compliance with the off-boarding toolkit.	7/1/2018	Adam Weikel, Assistant Vice President for Service
2017	2017-071	Complete Separating Employee Checklists Timely	VDOT	The Department has implemented an automated means for monitoring submission of separating employee checklists.	2/1/2018	Emily Elliott
2017	2017-072	Improve Controls over Payroll	DBHDS	The payroll test work was completed by the DBHDS Office of Internal Audit. In addition, the Department has agreed with the responses to the findings that were given by the four facilities where payroll test work was completed. The responses will satisfy the recommendations made in this finding.	9/1/2018	Randy Sherrod - Internal Audit Director

Fiscal Year	Final Finding No.	Title of Finding	State Agency	Initial Corrective Action	Estimated Completion Date	Responsible Contact Person
2017	2017-073	Improve Management Oversight of Wage Employee Timekeeping	VCU	VCU has a large number of employees with varying shifts as well as unique needs that require employees to work excess hours at times. Managers are ultimately responsible for reviewing, correcting and approving hours worked for their employees. In addition to managers, timekeepers, who have been trained on timekeeping and leave reporting policies as well as system notifications and reports, play a key role in assuring policy is enforced in the system. To supplement these controls, payroll is now using a report to identify hours worked over 12 hours in one day. The payroll department is contacting the managers of the employees with segments totaling over 12 hours before processing the payroll. Managers and timekeepers will also be reminded periodically to use the system-provided alerts and reports.	6/30/2018	Amy Barnes, Payroll Director
2017	2017-074	Comply with Commonwealth Requirements for Wage Employees	VCU	VCU HR will send another universal reminder regarding compliance with the laws, and the VCU HR Compliance Office will continue to monitor the quarterly hour reports. The VCU Compliance Office will direct the HR liaisons to immediately track and maintain a running account of any employee who looks to be close to 29 hours per week or who looks to be in potential violation of the 1500 annual hour limit. In the 2017-2018 reporting year, VCU HR will continue to send the report containing the names of employees who have exceeded 1,200 hours to the relevant HR liaisons, but the VCU HR Compliance Office will also communicate directly with HR Professionals any time an hourly or wage worker exceeds 1,200 hours in the reporting period and will direct the respective HR Professional overseeing the HR liaisons to more closely monitor the matter. The VCU HR Compliance Office will also discuss with the HR Professionals ways to incorporate measures within the schools and divisions to determine if hourly employees are working in multiple positions and engage them in discussing ways they can better manage this situation among the schools and divisions.	6/30/2018	Ishneila Moore, Director of Employee Relations and Performance Management
2017	2017-075	Comply with Commonwealth Requirements for Wage Employees	UVA/AD	The Human Resource department will reinforce Human Resource Policy 2.20 and the 1,500 hour rule to all departments. In addition, Payroll/Human Resources will implement additional controls to monitor non-benefit employees' hours and communicate employees approaching the annual limit to the respective department in a timely manner. In addition, the University is in the process of implementing a new HR management system, which will enable a more rigorous process to ensure termination takes place before the 1,500 hour threshold.	7/1/2018	John Kosky, Assistant Vice President for IMPACT and Decision Support
2017	2017-076	Comply with 1,500 Hour Rule for Wage Employees	DOC	The DOC HR Manager will develop a memorandum to alert all levels of staff of their responsibility to uphold the integrity of the 1,500 hours rule for wage employees. The memorandum will address supervisory accountability for maintaining hours within established thresholds. DOC will institute a maximum of 1,450 hours during the wage tracking year (May 1st through April 30th) for all wage employees. Any individual exception to work beyond the 1,450 hour threshold will require the approval of the respective Deputy Director or their appointed designee. Utilizing an appropriate database tracking method, wage employees reaching the 1,400 hour threshold will cease working until an audit of their hours by the facility and HQ HR designee confirms these hours. Once this has been done, the employee may continue to work up to the established DOC threshold of 1,450 hours. Supervisors who allow employees to exceed 1,450 hours will be subject to discipline under Standards of Conduct, and depending on the severity of the situation may be terminated for not following guidelines.	3/31/2018	Barry Elgert - Human Resource Manager
2017	2017-077	Improve Controls Over the Commonwealth's Retirement Benefits System	DBHDS	DBHDS will ensure that VNAV snapshot reconciliations are completed in a timely manner. In addition, policies and procedures will be enhanced to adequately describe how the reconciliations of FMS and CIPPS to VNAV are to be completed. DBHDS will also ensure that no employee has duplicate accounts in VNAV by reviewing the access levels in that system.	3/31/2018	Stacy Pendleton - DBHDS HR Manager Randy Sherrod - DBHDS Internal Audit Director

Fiscal Year	Final Finding No.	Title of Finding	State Agency	Initial Corrective Action	Estimated Completion Date	Responsible Contact Person
2017	2017-078	Continue to Improve Internal Controls over Retirement Contribution Reconciliations	VDOT	Human Resources will document and implement improved internal processes requiring: * Resolution of all reconciling items prior to the Department's monthly snapshot confirmation. This is already a requirement in the VDOT reconciliation process. If there are any complications preventing correction of errors due to unforeseen circumstances including system issues on the PMIS/DHRM or VRS/VNAV end, this will be documented and communicated with VRS prior to snapshot confirmation. * Retaining supporting documentation related to the cause of reconciling items, as well as the dates and methods of resolution. In December of 2017, VDOT added additional notes to the weekly reconciliation files detailing the fix required, who is responsible (VRS or VDOT HR or VDOT Payroll) and when it was corrected. This is now part of the documentation process moving forward. * Retaining a complete file for weekly reconciliations. In October of 2017, HR added a report that tracks the history of all VNAV errors that were corrected. This historical tracking will continue to be part of the process moving forward.	3/1/2018	Emily Elliott
2017	2017-079	Ensure all Nonexempt Active Vendors in the Commonwealth's Accounting and Financial Reporting System Have a Form W-9	DOA	DOA will run a system query to determine which active non-exempt vendors do not have Form W-9. Any vendor on this list that has not received a payment in the last 10 months will be inactivated. For the remainder of the vendors on the list DOA will contact both the vendor and the agencies making payments to them to obtain a Form W-9. If a Form W-9 is not received after 3 months of notification the vendor will be inactivated.	12/30/2018	Carlton McKinnon
2017	2017-080	Perform Adequate Due Diligence before Authenticating and Paying Vendors	DOE/COO	1) Develop and implement a review/approval process to determine legitimacy of vendor invoices, specifically vendor invoices for which no existing purchase order has been issued authorizing the delivery of services or goods. The implemented process will require all vendor billings to be validated by program offices as legitimate prior to continued routing for approvals and processing for payment. Suspicious transactions will require additional review by the Director of Procurement, the Director of Fiscal Services, and the Deputy of Finance and Operations. (IN PROGRESS) 2) Fiscal Services will conduct periodic training for all DOE employees. (IN PROGRESS/CONTINUOUS) 3) Procurement will conduct periodic training for all DOE employees. (IN PROGRESS/CONTINUOUS) 4) Business Risk Management will conduct periodic training for all DOE employees. (IN PROGRESS/CONTINUOUS)	6/30/2018	Christine Lopilato, Director of Fiscal Services Tom Broyles, Director of Business and Risk Management Marie Williams, Director of Procurement Program Office Directors
2017	2017-081	Create Policies and Procedures to Ensure Compliance with Statement of Economic Interest Requirements	DMAS	The Human Resources Division (HR) plans to take the following corrective actions: 1) Contact VA Ethics Council for updated guidance on system functionality since currently the Disclosure System cannot accept transfers within the Agency. Unless the system is unlocked, employees transferring to positions requiring completion of the SOEI, the coordinator cannot add them and initiate emails for completion of the Statement of Economic Interest forms. Estimated completion date: January 24, 2018; 2) Request from the Ethics Council and updated Users' Guide explaining the functionality of the system. Estimated completion date: January 8, 2018 [The Ethics Council was unable to provide updated Users Guide. HR will follow-up with new Ethics Council Coordinator.]; and 3) Write internal procedures for DMAS. The following controls have been implemented: 1) Requests to Fill documents include a check off box for Statements of Economic Interest to ensure positions are added to the list to be added to the Disclosure System; 2) HR staff reviews all positions when staffing changes are announced. Employment Manager and HR Analysts notify the HR Director when required positions are filled; and 3) HR Director receives notification from the Operations Manager of the new staff member's personal email address since DMAS email addresses are not set until an employee arrives and the Disclosure System cannot operate without an email address.	3/31/2018	Kathleen Guinan, DMAS Human Resources Director, Human Resources Division

Fiscal Year	Final Finding No.	Title of Finding	State Agency	Initial Corrective Action	Estimated Completion Date	Responsible Contact Person
2017	2017-082	Obtain and Retain Statement of Economic Interest Training Records	DSS	DSS will use the Commonwealth of Virginia Learning Center (COVLC) to obtain and retain Statement of Economic Interest (SOEI) training records. Training records will be maintained in the COVLC for perpetuity, satisfying the minimum five-year retention requirement. Should the current COVLC be replaced by a new system or platform, DSS will ensure that all historical SOEI training records are migrated to the new COV learning system. DSS will use the Office of Attorney General's SOEI training module, deemed acceptable by the Ethics Council. The SOEI training content has been loaded into the COVLC. The DSS SOEI Coordinator notified all DSS employees within positions of trust to complete the required SOEI training by January 5, 2018. DSS has also obtained the SOEI training attendance records for DSS employees from The Ethics Council. These records have been updated and are now available in the COVLC. Going forward, DSS will use the e-mail notification features of the COVLC to ensure that DSS employees within positions of trust are notified to take their required SOEI training every 24 months. At least 60 days in advance of their two-year training period expiration date, employees within positions of trust will be notified by email that they must take SOEI training again. New employees will continue to be notified of the SOEI training requirement during their recruitment, and will be configured in the COVLC during on-boarding, and complete SOEI training as required. These actions have been documented into the SOEI Procedures within the Division of Organizational Development. The procedure documents are maintained by and have been implemented by the DSS SOEI Coordinator.	6/30/2018	Stephanie Larson
2017	2017-083	Improve Controls Over Building and Grounds Inventory at Fluvanna Correction Center for Women	DOC	FCCW's Building and Grounds (B&G) staff will update the inventory items and ensure the most current purchase amounts are entered. The B&G Superintendent has been trained to review and complete all adjustments in the TMS inventory management system and will ensure all inventory is entered correctly into TMS and has supporting documentation. Additionally, the B&G Superintendent will ensure the storeroom door remains secured and controlled at all times by limiting access to one key with an electronic box. Staff will be instructed on the requirement to keep the storeroom door secure. Key access will be restricted to the B&G department and only authorized staff will receive access within the key watch system. All new staff will receive TMS training within 90 days of employment. Monthly trade workers will conduct and document monthly audits of inventory items in their area of responsibility. The B&G Superintendent will conduct monthly spot checks of all items in the storeroom checking a minimum of 3 items per page.	6/30/2018	David Baker - FCCW B&G Superintendent Jeffrey Snoddy - FCCW Assistant Warden

Fiscal Year	Final Finding No.	Title of Finding	State Agency	Initial Corrective Action	Estimated Completion Date	Responsible Contact Person
2017	2017-084	Improve the Accounts Receivable Collection Process	DMAS	The untimely and inaccurate processing of accounts receivable transactions is directly associated with the delayed automation in overpayment processing, backlog of receivables, and the lack of appropriate resources to focus earnestly on collection efforts. The Current Agency Accounting System upgrade was successfully implemented November 13, 2017. All divisional efforts were focused on the implementation of the Current Agency Accounting System upgrade thereby causing delays in projected enhancements to Accounts Receivable. Divisional resources will also focus efforts on the implementation of the New Claims Processing Systems for financial systems and data warehouse. The areas of greatest challenge are heavily entrenched in manual processes. Among these manual processes is Program Integrity's notification of recipient excess benefits. An automation project is in early development that will allow for automatic notifications and automatic retrieval of information needed to establish the receivable. Therefore, DMAS will continue to work with the Information Management Division to implement those enhancements DMAS is able to do amidst projects with a higher priority. Thus expected Fiscal AR automation will be completed by September 30, 2018. Fiscal AR is committed to improving the accounts receivable collection process and reducing the backlog of receivables. Therefore, with management approval, Fiscal AR will temporarily augment resources to effectively right-size the workload which will directly impact the reduction of the backlog and improve the timeliness in collection efforts. Increase resources are expected to be in place by June 30, 2018.	12/31/2018	Karen Stephenson, Controller, DMAS Fiscal Division
2017	2017-085	Establish Sound Budgetary Controls over Disbursements	DOE/COO	<p>1) Work with EIM to determine cause of budget controls failure in OMEGA, resulting in overpayment to sub-recipient. (COMPLETED 12/2017)</p> <p>2) Work with EIM to ensure hard-coded calculation in OMEGA for available grants balances is modified to include payments "Approved for Payment" and "Paid" status. When claims are "Approved for Payment" but not yet marked as "Paid", the hard-coded calculation in OMEGA must include the "Approved for Payment" claims (treated as encumbrances against the available grants balances) to ensure proper calculation of available remaining balances. Fiscal Services will work with EIM to communicate Fiscal Services needs, and test solutions prior to being placed in Production. (IN PROGRESS)</p> <p>3) Fiscal Services will conduct Program Managers' Training, which will include a topic refresher for all Program Offices staff to vigilantly monitor their sub-recipients' grant award balances in OMEGA. Program Offices will be strongly encouraged to perform (at least) quarterly analyses of sub-recipient grant award balances to OMEGA grant payments and OMEGA grant award remaining balances to identify any irregularities or errors requiring correction. (IN PROGRESS)</p>	6/30/2018	Christine Lopilato, Director of Fiscal Services Bobby Keener, Director of EIM & Technology Innovations Program Office Directors Responsible for Federal Funding

Fiscal Year	Final Finding No.	Title of Finding	State Agency	Initial Corrective Action	Estimated Completion Date	Responsible Contact Person
2017	2017-086	Drawdown Federal Grant Funds as Instructed and Update Loan Request with Important Facts	DOE/COO	<p>1) Develop New Grant Program Application Approval Form to be completed by Program Offices to ensure proper notification of new sources of federal grant funding being received by DOE (other than USED and USDA). Part A of the form will be routed by the Program Office with all required supporting documentation prior to grant applications being submitted to awarding entities for consideration; Part B of the form will be routed by the Program Office upon notification of grant funding, ensuring proper follow-up for grant terms and instructions including Fiscal Services drawdown access accounts (other than existing/recurring USED and USDA grant awards), and acknowledgment by Program Offices of responsibilities for financial reporting. (COMPLETED 3/2017; IMPLEMENTED 8/2017)</p> <p>2) Improve Fiscal Services processes and documented SOPs to include immediate notification to the Director and Associate Director for any federal payments made for which immediate drawdown has not been made, including explanation/justification for delay in drawdowns. (IN PROGRESS)</p> <p>3) Enforce existing Fiscal Services internal controls process that requires monthly analysis of federal expenditures and revenues to ensure federal expenditures are being drawdown timely, and revenues are being recorded timely. Any variances or gaps between federal expenditures and revenues must be researched and documented. Monthly analyses will be performed by the Senior Compliance and Reporting Specialist, reviewed by the General Ledger Manager, with final review by the Director and/or Associate Director. (IN PROGRESS)</p> <p>4) Provide Department of Accounts with explanation for why DOE was placed in restricted status with HHS (SAMHSA), resulting in the request for the Treasury Loan of \$1.6 million. (COMPLETED 12/2017)</p>	6/30/2018	Christine Lopilato, Director of Fiscal Services
2017	2017-087	Match Federal Grants with Qualifying State Expenses	VSU	VSU submitted a formal response to the USDA/NIFA final report on August 4, 2017. VSU is still awaiting an official response from USDA/NIFA to the repayment request and the corrective actions cited in the 2014 final report. On August 17, 2017 VSU visited with USDA/NIFA staff in Washington, D.C. to discuss proposed fiscal policy and procedure changes. VSU has since implemented changes that will prevent any occurrences cited in the 2014 review. VSU is preparing a formal request to the USDA/NIFA Grants Award Division to return 2015 and 2016 state matching funds previously used for unallowable indirect cost recoveries (Section 1444 and 1445 – Research & Extension) to VSU/CEAR to implement new research and extension programs to the public through the newly established Center for Agricultural Research, Engagement and Outreach.	3/1/2018	Dr. G. Dale Wesson, VP for Research and Economic Dev. Dr. M. Omar Faison, Assistant VP for Research and Office of Sponsored Research Programs (OSRP)
2017	2017-088	Strengthen Subrecipient Monitoring Process	VDH	For Program year 2016-2017, the sponsor profile rolled over from program year 2015-2016 with a packet status of Not Submitted. Because the information was in Not Submitted status, the New Application Report would not have pulled this particular organization. VDH has since implemented a solution by including a Packet Original Approval Date for the master sponsor packet regardless of the status of different components of the application. The sponsor has been scheduled for an administrative review.	11/16/2017	Mandeep Virk-Baker, Community Nutrition Division Director
2017	2017-089	Improve Controls over Federal Reporting	VSBFA	Implement a formal review process of the E0209 federal financial report by realigning the responsibility for preparation of the report and by insuring the report has dual, formal review by senior VSBFA accounting staff and by the VSBFA Chief Credit Officer, or by senior VSBFA accounting staff and the VSBFA Executive Director. Implement detailed internal policies and procedures for the preparation of the ED209 report to insure accuracy of all financial metrics, including those specific to this report. Insure sufficient staff resources and training related to the report preparation. Consideration is being given to the creation of an additional VSBFA staff position devoted to Reporting and Compliance. Improve internal financial reports related to the preparation of the ED209 report to insure adequate support for all financial metrics specific to the ED209 report.	4/30/2018	Anna MacIdey, Interim Executive Director and Chief Credit Officer

Fiscal Year	Final Finding No.	Title of Finding	State Agency	Initial Corrective Action	Estimated Completion Date	Responsible Contact Person
2017	2017-090	Strengthen Internal Controls over Federal Awards	DMA	Correctly classify National Guard Military Operations and Maintenance federal program to the correct CFDA number. Develop comprehensive policy and procedure to allocate payroll costs by program, project, or facility. Develop master list of all agency contracts, including the initial period and renewals. Agency has requested guidance for using a tool within eVA for this purpose. Conduct agency-level and transaction-level risk assessments.	9/30/2018	Steve Arthur Don Sutherland Beth Easter JT Palmore
2017	2017-091	Comply with Statewide and Agency Procurement Policies and Procedures	DMA	Ensure automated date stamps are available in each department that receive bids/RFP's. Ensure a copy of bids are posted in a public area normally used by the agency for such notices. Establish an SOP for placement of such information.	3/31/2018	Beth Easter
2017	2017-092	Develop Procedures and Performance Expectations for Resolving Social Security Number Discrepancies	DMAS	Steps to be taken or that have been taken: 1) Provide DSS with a copy of the RS-O-485A report each month (For years, the Current Claims Processing System generated the RS-O485A report and it was sent to DSS. However, the report did not contain the correct recipients. It contained Medicaid recipients and GAP cases but not FAMIS/FAMIS MOMS recipients. DSS did not need the GAP cases but needed the Medicaid and FAMIS/FAMIS MOMS recipients. In March 2017, DMAS updated the RS-O-485A report to include both the Medicaid and FAMIS/FAMIS MOMS recipients began sending the report each month to DSS. The March 2017 report included enrollment for January through March 2017. For the current process, the Office of Data Analytics generates the report and sends electronically to DSS. DMAS is in the process of revising the RS-O-485A report so that the Current Claims Processing System will automatically generate the monthly report to include all Medicaid and FAMIS recipients (and not GAP cases) and automatically send it to DSS.); 2) Monitor completion of the RS-O-485A report each month (Staff in the Enrollment Unit within the Division of Eligibility and Enrollment Services will monitor the report on a monthly basis to ensure that action has been taken to correct Social Security Numbers in the system. This action will begin in February 2018 and will be an ongoing monthly process. SSNs found to remain on the report and not corrected will be routed to the appropriate Virginia Department of Social Services Regional Medicaid Consultant for correction and provided to the Virginia Department of Social Services Medical Assistance Unit Manager.); 3) Develop and implement policies, procedures and baseline performance measures related to Social Security numbers in the Current Claims Processing System: a) While there are policies and procedures related to verification of Social Security numbers already set out in the Medicaid eligibility manual, DMAS Eligibility and Enrollment Services Division staff will work with staff from the Virginia Department of Social Services Medical Assistance Unit to implement these new procedures no later than July 2018 and will develop procedures for monitoring performance by local agencies no later than that date as well.	7/1/2018	Cindy Olsen, Division Director, Eligibility and Enrollment Services Division
2017	2017-093	Complete Risk Assessments for Subrecipients	DCJS	To ensure compliance with new VOCA rules and sub-recipient monitoring under the Federal Uniform Guidance, DCJS Victims Services staff, in collaboration with Grants Administration, have drafted a Crime Victim Services Monitoring Plan and Policy, which includes the use of a formal, scored, risk assessment instrument and written documentation of the assessment results. The Crime Victim Services Monitoring Plan and Policy will be implemented prior to the next funding cycle of sub-recipients. In an effort to stay abreast of changes or updates, Victims Services and Grants Administration staff will receive ongoing training on the Uniform Guidance requirements for sub-recipient monitoring. Additionally, to ensure continued compliance and promote consistency, two full-time Victims Services grant monitor positions are currently in recruitment. The addition of these positions, and adoption of an updated agency monitoring plan and policies, will increase DCJS capacity to conduct on-site monitoring, guided by the formal, scored, risk assessment tool. The Division Directors of Finance and Administration and Programs and Services will ensure adherence to the <i>Crime Victim Services Monitoring Plan and Policy</i> .	7/1/2018	John Colligan, Division Director of Finance and Administration Thomas Fitzpatrick, Division Director of Programs and Services Kay Bullock, Manager, Victims Services

Fiscal Year	Final Finding No.	Title of Finding	State Agency	Initial Corrective Action	Estimated Completion Date	Responsible Contact Person
2017	2017-094	Improve Internal Controls over Financial Reporting	DCJS	DCJS has developed a review process to ensure that similar errors will not occur in the future. The quarterly federal financial reports submitted to the Department of Justice will be reviewed for accuracy and initialed by the preparer. The Manager of Grants Administration will then review and initial the reports. The Division Director of Finance and Administration will ensure compliance with this new process which will be immediately implemented.	2/7/2018	John Colligan, Division Director of Finance and Administration Albert Stokes, Manager, Grants Management
2017	2017-095	Update Contract Provisions, Enforce Contract Administration, and Evaluate Supporting Documentation and Reasonableness of Federal Grant Expenditures	VSU	The Office of Sponsored Research and Programs (OSRP) will develop procedures and processes for Principal Investigators (PI) to confirm that goods and services were received and that work performed by contractors has been completed prior to providing approval of payment to Accounts Payable. OSRP will work with the offices of Grants & Contracts and Accounts Payable to develop training to ensure PIs are knowledgeable about invoice requirements.	3/1/2018	Dr. G. Dale Wesson, VP for Research and Economic Dev Kevin Davenport, VP for Finance Dr. Jewel Bronaugh, Director of Center for Agricultural Research, Engagement and Outreach