DEPARTMENT OF JUVENILE JUSTICE

INTERNAL CONTROL QUESTIONNAIRE REVIEW RESULTS AS OF FEBRUARY 2024

Auditor of Public Accounts
Staci A. Henshaw, CPA
www.apa.virginia.gov
(804) 225-3350

- TABLE OF CONTENTS -

Commonwealth of Virginia

Auditor of Public Accounts

Staci A. Henshaw, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

March 25, 2024

Amy Floriano, Director
Department of Juvenile Justice
600 East Main Street
Richmond, Virginia 23219

INTERNAL CONTROL QUESTIONNAIRE REVIEW RESULTS

We have reviewed the Internal Control Questionnaire for the **Department of Juvenile Justice** (Juvenile Justice). We completed the review on February 14, 2024. The purpose of this review was to evaluate if the agency has developed adequate internal controls over significant organizational areas and activities and not to express an opinion on the effectiveness of internal controls. Management of Juvenile Justice is responsible for establishing and maintaining an effective control environment.

Review Process

During the review, the agency completes an Internal Control Questionnaire that covers significant organizational areas and activities including payroll and human resources; revenues and expenses; procurement and contract management; capital assets; grants management; debt; and information technology and security. The questionnaire focuses on key controls over these areas and activities.

We review the agency responses and supporting documentation to determine the nature, timing, and extent of additional procedures. The nature, timing, and extent of the procedures selected depend on our judgment in assessing the likelihood that the controls may fail to prevent and/or detect events that could prevent the achievement of the control objectives. The procedures performed target risks or business functions deemed significant and involve reviewing internal policies and procedures. Depending on the results of our initial procedures, we may perform additional procedures including reviewing evidence to ascertain that select transactions are executed in accordance with the policies and procedures and conducting inquiries with management. The "Review Procedures" section below details the procedures performed for Juvenile Justice. The results of this review will be included within our risk analysis process for the upcoming year in determining which agencies we will audit.

Review Procedures

We evaluated the agency's corrective action for the 2020 internal control questionnaire review findings as well as the findings in the report titled "Cycled Agency Information Systems Security Review for the year ended June 30, 2020." The agency has taken adequate corrective action with respect to findings reported in the prior review and audit that are not repeated in the "Review Results" section below.

We reviewed a selection of system and transaction reconciliations in order to gain assurance that the statewide accounting system contains accurate data. The definitive source for internal control in the Commonwealth is the Agency Risk Management and Internal Control Standards (ARMICS) issued by the Department of Accounts (Accounts); therefore, we also included a review of ARMICS. The level of ARMICS review performed was based on judgment and the risk assessment at Juvenile Justice. Our review of Juvenile Justice's ARMICS program included a review of all current ARMICS documentation and a comparison to statewide guidelines established by Accounts. Further, we evaluated the Juvenile Justice's process of completing and submitting attachments to Accounts.

We reviewed the Internal Control Questionnaire and supporting documentation detailing policies and procedures. As a result of our review, we performed additional procedures over the following areas: payroll and human resources; revenues and expenses; procurement and contract management; capital assets; and information technology and security. These procedures included validating the existence of certain transactions; observing controls to determine if the controls are effectively designed and implemented; reviewing transactions for compliance with internal and Commonwealth policies and procedures; and conducting further review over management's risk assessment process.

As a result of these procedures, we noted areas that require management's attention. These areas are detailed in the "Review Results" section below.

Review Results

We noted the following areas requiring management's attention resulting from our review:

- **Repeat -** Juvenile Justice continues not to formally review information system audit records for each of its sensitive systems monthly and document the results in accordance with its Information Technology (IT) Security Audit, Monitoring, and Logging Policy (Policy), which is based on the Commonwealth's Information Security Standard, SEC 501 (Security Standard). Further, Juvenile Justice does not enforce separation of duties within its policy by requiring the system administrator to review and analyze information system audit records, which includes their own activity. Juvenile Justice should revise its policy to enforce separation of duties when reviewing audit log information. Additionally, Juvenile Justice should dedicate the necessary resources to implement a formal process to review and analyze information system audit records at least every 30 days for all sensitive information systems to monitor for indications of inappropriate or unusual activity. To assist with this formal process, Juvenile

Justice should consider the acquisition of an automated tool to help with the review and analysis of information system audit records.

- **Partial Repeat -** Juvenile Justice continues to not properly maintain information technology risk management and contingency planning documentation in accordance with its IT Contingency Planning Policy and IT Risk Assessment Policy, which are both based on the Security Standard. While Juvenile Justice resolved three of the five findings from the 2019 fiscal year audit, two weaknesses continue to exist. Juvenile Justice continues not to have risk assessments for any of their four sensitive systems. In addition, Juvenile Justice continues not to have an IT Disaster Recovery Plan (IT DRP). Juvenile Justice should perform and document IT risk assessments for all Juvenile Justice's sensitive systems at least once every three years. Juvenile Justice should then review the risk assessment results on an annual basis and make changes if necessary. Additionally, Juvenile Justice should develop and maintain an IT DRP based on the continuity plan which supports the restoration of essential business functions and dependent business functions, and periodically review, reassess, test, and revise the IT DRP to reflect any possible changes in Juvenile Justice's IT environment.

- **Repeat -** Juvenile Justice continues not to appropriately manage systems access in accordance with its IT Logical Access to Computer Systems Policy (Logical Access Policy), which is based on the Security Standard. Specifically, Juvenile Justice continues not to perform an annual review of systems access. Juvenile Justice does not have a formal process in place to ensure it performs the required annual review of systems access. In addition, Juvenile Justice continues not to have an adequate termination process in place to disable systems access within 24 hours of employee termination as required by its Logical Access Policy and the Security Standard. Juvenile Justice did not retain appropriate documentation to indicate that it disabled access within 24 hours of termination for 39 of the 40 (97%) sampled terminated employees. For the one remaining employee, Juvenile Justice did not disable access within 24 hours of termination. Juvenile Justice should improve and follow its process to ensure it disables information system access for terminated employees within 24 hours as required by the Security Standard and retain the necessary documentation. Juvenile Justice should then develop and implement a formal process to perform annual reviews of systems access as required by the Security Standard and its Logical Access Policy.

- **Partial Repeat -** Juvenile Justice continues to not meet certain requirements of the Security Standard, the Commonwealth's Security Awareness Training Standard, SEC 527 (Security Awareness Training Standard), as well as its Security Awareness Training policy (Security Awareness Policy). Specifically, Juvenile Justice does not have an adequate process in place to ensure all users complete security awareness training, resulting in 87 of the 1,337 (6.5%) users assigned the training not completing the training during fiscal year 2022. In addition, when users do not complete training, Juvenile Justice does not revoke the user's access or implement other enforcement measures. Juvenile Justice developed and implemented a

process to assign security awareness training to its employees. However, Juvenile Justice relies upon employee supervisors and managers to enforce completion of the training. Juvenile Justice should implement a formal process to monitor and enforce security awareness training within 30 days of employment and on an annual basis thereafter.

- **Repeat -** Juvenile Justice continues to not adequately review and update their IT policies and procedures. Juvenile Justice reviewed their policies and procedures in August and September of 2020, but has not conducted a review since 2020. The Security Standard requires that agencies perform a review and update of IT policies and procedures on an annual basis, or more frequently if required to address an environmental change. Juvenile Justice should develop a process to consistently review and update IT policies and procedures on an annual basis, or more frequently to address an environmental change, which will help ensure the confidentiality, availability, and integrity of Juvenile Justice's environment.

- **Repeat –**Juvenile Justice has formal, documented policies and procedures over many of its significant business processes. However, during our review, we identified several business areas where Juvenile Justice should develop or update policies and procedures to maintain an effective control environment. The Commonwealth Accounting Policies and Procedures (CAPP) Manual Topic 20905 and other sections of the CAPP Manual require each agency to "publish its own policies and procedures documents, approved in writing by agency management." Management should ensure detailed policies and procedures exist for all critical business areas. In addition, management should continue to develop a process to review and approve all policies and procedures either annually or as needed and maintain documentation of the process.

- **Repeat –** Juvenile Justice's ARMICS process does not meet the minimum requirements set by Accounts. Specifically, Juvenile Justice does not have a complete agency-level risk assessment. Juvenile Justice has already submitted a corrective action plan covering this issue. Additionally, Juvenile Justice should document their risk assessment and testing of controls for their financial reporting processes and consider the risk of fraud in all relevant fiscal processes. Juvenile Justice should ensure the ARMICS process and documentation meets all the minimum requirements issued by Accounts.

- **Repeat** – Juvenile Justice does not ensure that employees who file Statements of Economic Interest forms take the required training every two years. We noted one out of three employees selected did not complete the required training within the two-year timeframe. Section 2.2-3128 of the Code of Virginia requires state filers to complete an orientation ethics course every two calendar years. Juvenile Justice should ensure that the employees who file Statement of Economic Interest forms complete the training semi-annually as required.

- **Partial Repeat** – Juvenile Justice did not implement corrective action from a previous review by evaluating a Service Organization Control (SOC) report for the administrator of its healthcare benefits program for direct-care youth. CAPP Manual Topic 10305 requires agencies to maintain oversight over third-party service providers and provide the Commonwealth assurance over outsourced operations. Juvenile Justice should evaluate SOC reports for all significant third-party service providers.

- Juvenile Justice did not properly identify and account for leases in accordance with the CAPP Manual and Governmental Accounting Standards Board (GASB) Statement No. 87. Juvenile Justice recorded leases they should not have, potentially causing duplicate lease information within the Commonwealth's Annual Comprehensive Financial Report. Juvenile Justice also did not properly evaluate and record the group of leased assets with the same contracted vendor, lease term, and interest rate. In addition, Juvenile Justice did not follow the correct procedure to determine the interest rate. CAPP Manual Topic 31200, which references GASB Statement No. 87, requires agencies to properly identify leases and group leases for recording in the lease accounting system to ensure proper classification of long-term and short-term, and to evaluate explicit, implicit, and incremental borrowing rates before defaulting to the prime rate for a reasonable and accurate interest rate. Management should update lease processes and ensure it properly records and classifies leases.

- Juvenile Justice's procedures on employee separations include a checklist to ensure the proper documentation for an employee that has separated from the agency. However, Juvenile Justice was unable to provide supporting documentation showing management completed this checklist for two out of four (50%) employees reviewed. Juvenile Justice should ensure it is completing the employee separations checklist and retaining this documentation for off-boarding employees.

- Juvenile Justice did not maintain documentation showing supervisors granted approval prior to employees working overtime. For one of four employees reviewed, there was no evidence that supervisors approved the overtime worked. Juvenile Justice should ensure that employees receive the proper approval for overtime prior to the employee working overtime and retain evidence of this approval.

We discussed these matters with management on August 1, 2023, and February 14, 2024. Management's response to the findings identified in our review is included in the section titled "Agency Response." We did not validate management's response and, accordingly, cannot take a position on whether or not it adequately addresses the issues in this report. Certain information, marked with a

black box, was redacted from the response as the information is Freedom of Information Act Exempt under § 2.2-3705.2 of the Code of Virginia, due to it containing descriptions of security mechanisms. This report is intended for the information and use of management. However, it is a public record and its distribution is not limited.

Sincerely,

Staci A. Henshaw
Auditor of Public Accounts

JDE/vks

Amy M. Floriano
Director

Dale L. Holden, Jr.
Chief Deputy Director

COMMONWEALTH OF VIRGINIA

Department of Juvenile Justice

P.O. Box 1110
Richmond, VA 23218
(804) 371.0700
Fax: (804) 371.6497
www.djj.virginia.gov

April 1, 2024

Staci A. Henshaw, CPA, CGMA
Auditor of Public Accounts
101 North 14th Street, 8th Floor
Richmond, VA 23219

Dear Ms. Henshaw:

I extend my gratitude and appreciation for the professionalism demonstrated by the Auditor of Public Accounts (APA) staff assigned to the Department of Juvenile Justice (DJJ) audit. We thank you for alerting us to these deficiencies and please know that all your findings are being taken seriously. All DJJ staff support my efforts to ensure these findings are resolved in an effective and efficient manner. Following our analysis of the FY22 ICQ Review Results for DJJ, we have summarized each finding and provided responses to demonstrate actions taken to resolve these issues and ensure compliance.

Our responses are noted below.

Review Results

1. **Repeat -** Juvenile Justice continues not to formally review information system audit records for each of its sensitive systems monthly and document the results in accordance with its Information Technology (IT) Security Audit, Monitoring, and Logging Policy (Policy), which is based on the Commonwealth's Information Security Standard, SEC 501 (Security Standard). Further, Juvenile Justice does not enforce separation of duties within its policy by requiring the system administrator to review and analyze information system audit records, which includes their own activity. Juvenile Justice should revise its policy to enforce separation of duties when reviewing audit log information. Additionally, Juvenile Justice should dedicate the necessary resources to implement a formal process to review and analyze information system audit records at least every 30 days for all sensitive information systems to monitor for indications of inappropriate or unusual activity. To assist with this formal process, Juvenile Justice should consider the acquisition of an automated tool to help with the review and analysis of information system audit records.

Response
DJJ acknowledges the need to formally review system audit records and logs. The IT team began a manual process in 2023 to review all system logs and audit for the [redacted] system, however that was not sustainable due to the manual nature of the process. With VITA's acquisition in 2023 of a security information and event management application ([redacted]) that manages, imports, and analyses all machine and agency generated data, an automated process became available with a reasonable cost structure. In 2024 this application was opened to agency ISOs for first testing and implementation, and currently there is an enterprise project underway to begin importing all agency application log and application data. This project, and DJJ's active involvement in it, will allow DJJ to have an automated process to review, analyze, and audit all our [redacted] data in a replicable and formalized manner. This system will also allow DJJ to respond to unusual or potential security incidents as events and data are analyzed. This is a brand-new system for both DJJ and the Commonwealth and requires internal, dedicated resources for DJJ to implement and operate effectively and sustainably. DJJ's meeting with VITA service owner and internal DJJ resources is scheduled for April 8, 2024. This meeting will establish the timeline for routine oversight and analysis.

2. **Partial Repeat** - Juvenile Justice continues to not properly maintain information technology risk management and contingency planning documentation in accordance with its IT Contingency Planning Policy and IT Risk Assessment Policy, which are both based on the Security Standard. While Juvenile Justice resolved three of the five findings from the 2019 fiscal year audit, two weaknesses continue to exist. Juvenile Justice continues not to have risk assessments for any of their four sensitive systems. In addition, Juvenile Justice continues not to have an IT Disaster Recovery Plan (IT DRP). Juvenile Justice should perform and document IT risk assessments for all Juvenile Justice's sensitive systems at least once every three years. Juvenile Justice should then review the risk assessment results on an annual basis and make changes if necessary. Additionally, Juvenile Justice should develop and maintain an IT DRP based on the continuity plan which supports the restoration of essential business functions and dependent business functions, and periodically review, reassess, test, and revise the IT DRP to reflect any possible changes in Juvenile Justice's IT environment.

   Response
   DJJ acknowledges the need for regular reviews and updates to our risk management and contingency planning documentation. To address this oversight, DJJ has recently engaged Assura Inc to assist DJJ with a comprehensive review and update of our risk management and contingency planning documentation to comply with SEC530. Updated risk management and contingency planning documents are anticipated to be completed by September 4, 2024.

3. **Repeat -** Juvenile Justice continues not to appropriately manage systems access in accordance with its IT Logical Access to Computer Systems Policy (Logical Access Policy), which is based on the Security Standard. Specifically, Juvenile Justice continues not to perform an annual review of systems access. Juvenile Justice does not have a formal process in place to ensure it performs the required annual review of systems access. In addition, Juvenile Justice continues not to have an adequate termination process in place to disable systems access within 24 hours of employee termination as required by its Logical Access Policy and the Security Standard. Juvenile Justice did not retain appropriate documentation to indicate that it disabled access within 24 hours of termination for 39/40 (97%) sampled terminated

employees. For the one remaining employee, Juvenile Justice did not disable access within 24 hours of termination. Juvenile Justice should improve and follow its process to ensure it disables information system access for terminated employees within 24 hours as required by the Security Standard and retain the necessary documentation. Juvenile Justice should then develop and implement a formal process to perform annual reviews of systems access as required by the Security Standard and its Logical Access Policy.

Response

In January 2024, DJJ began a system wide review of all active accounts for DJJ's main sensitive system, [redacted]. This process is reviewed by all supervisors, the Data Integrity Unit (data owner), and IT to ensure that all active accounts are both necessary for that position, and that the access levels for each account are necessary to complete their position functions. This project has an estimated length of 3-4 months and will be an annual process moving forward. Since this is the first system-wide review of account access, there was a longer timeline. Each subsequent year will have shorter completion timelines as the overall process is streamlined. Data owner submission of changes to user accounts is expected to be delivered to IT in mid-April.

As new sensitive systems are brought online for DJJ, both business system owners and data owners are identified at the beginning of the project to ensure that account reviews are conducted for all systems on an annual basis.

4. **Partial Repeat -** Juvenile Justice continues to not meet certain requirements of the Security Standard, the Commonwealth's Security Awareness Training Standard, SEC 527 (Security Awareness Training Standard), as well as its Security Awareness Training policy (Security Awareness Policy). Specifically, Juvenile Justice does not have an adequate process in place to ensure all users complete security awareness training, resulting in 87 of the 1,337 (6.5%) users assigned the training not completing the training during fiscal year 2022. In addition, when users do not complete training, Juvenile Justice does not revoke the user's access or implement other enforcement measures. Juvenile Justice developed and implemented a process to assign security awareness training to its employees. However, Juvenile Justice relies upon employee supervisors and managers to enforce the completion of the training. Juvenile Justice should implement a formal process to monitor and enforce security awareness training within 30 days of employment and on an annual basis thereafter.

Response

In 2023, DJJ joined other Executive Branch agencies in the implementation of the KnowBe4 information security awareness training platform. This implementation has already seen improvements in the compliance of end user information security awareness training. DJJ now has the ability to assign and track new user security awareness training during the first 30 days after on-boarding, and annually thereafter. The next steps in this compliance effort include plans for account access revocation if training is not completed with the first quarter of the calendar year 2024 training campaign. The ISO will report all non-compliant accounts on or around 4/1/24 to senior leadership for review and approval of account revocation. The expectation is once agency culture changes regarding information security awareness training compliance, 100% compliance will be attainable. Current security awareness training for calendar year 2023 was completed with a 93.5% completion rate.

5. **Repeat -** Juvenile Justice continues to not adequately review and update their IT policies and procedures. Juvenile Justice reviewed their policies and procedures in August and September of 2020, but has not conducted a review since 2020. The Security Standard requires that agencies perform a review and update of IT policies and procedures on an annual basis, or more frequently if required to address an environmental change. Juvenile Justice should develop a process to consistently review and update IT policies and procedures on an annual basis, or more frequently to address an environmental change, which will help ensure the confidentiality, availability, and integrity of Juvenile Justice's environment.

   Response
   DJJ acknowledges the need for regular reviews and updates to our information security policies and procedures. In an effort to address this oversight, DJJ has recently engaged Assura, Inc. to assist DJJ with a comprehensive review and update of the information security program documents to comply with SEC530. Assura is actively engaged, and a kickoff meeting was completed March 4, 2024. Updated information security program documents are anticipated to be completed within approximately 60 days after project start.

6. **Repeat –**Juvenile Justice has formal, documented policies and procedures over many of its significant business processes. However, during our review, we identified several business areas where Juvenile Justice should develop or update policies and procedures to maintain an effective control environment. The Commonwealth Accounting Policies and Procedures (CAPP) Manual Topic 20905 and other sections of the CAPP Manual require each agency to "publish its own policies and procedures documents, approved in writing by agency management". Management should ensure detailed policies and procedures exist for all critical business areas. In addition, management should continue to develop a process to review and approve all policies and procedures either annually or as needed and maintain documentation of the process.

   Response
   DJJ has been actively reviewing, updating, and publishing internal policies and procedures. It is our mission to ensure all policies have been updated no later than the end of this fiscal year. Going forward, all policies and procedures will be reviewed, at a minimum, annually or more frequently if revisions are needed. In addition, the Administration and Finance division has been preparing desk procedures for all critical business areas. At this time, drafts have been prepared for over 75% of the critical business processes identified. They will be reviewed, revised if needed, and approved by June 30, 2024. Like the DJJ Policies and Procedures, the desk procedures will also be reviewed, at a minimum, annually or more frequently if revisions are needed.

7. **Repeat –** Juvenile Justice's ARMICS process does not meet the minimum requirements set by Accounts. Specifically, Juvenile Justice does not have a complete agency-level risk assessment. Juvenile Justice has already submitted a corrective action plan covering this issue. Additionally Juvenile Justice should document their risk assessment and testing of controls, for their financial reporting processes and consider the risk of fraud in all relevant fiscal processes. Juvenile Justice should ensure the ARMICS process and documentation meets all the minimum requirements issued by Accounts.

Response
DJJ has completed and documented the agency level risk assessment and the final Corrected Action Plan was submitted DOA in October 2023. DOA contacted us last week with additional questions and DJJ's internal auditor promptly responded. DJJ currently utilizes a third-party vendor to perform our ARMICS review. Risk and fraud are tested and documented for financial reporting in all relevant fiscal processes.

8. **Repeat** – Juvenile Justice does not ensure that employees who file Statements of Economic Interest forms take the required training every two years. We noted one out of three employees selected did not complete the required training within the two-year timeframe. Section 2.2-3128 of the Code of Virginia requires state filers to complete an orientation ethics course every two calendar years. Juvenile Justice should ensure that the employees who file Statement of Economic Interest forms complete the training semi-annually as required.

   Response
   DJJ reviewed the existing process and made significant changes to ensure the agency came into and remains compliant with the annual filing and required training within the two-year timeframe. DJJ evaluated all employee positions and reviewed employee work profiles (EWP) to identify and confirm their duties fell within the guidelines of the Executive Order for SOEI requirement. We immediately worked with the identified employees to complete the required training and became 100% compliant as of February 1, 2024. DJJ has established a roster of all positions required to file for tracking purposes. We continue to work with the Council and have established the "trigger" reminders through their website. We are also confirming training completion through the Commonwealth of Virginia Learning Center.

9. **Partial Repeat** – Juvenile Justice did not implement corrective action from a previous review by evaluating a Service Organization Control (SOC) report for the administrator of its healthcare benefits program for direct-care youth. CAPP Manual Topic 10305 requires agencies to maintain oversight over third-party service providers and provide the Commonwealth assurance over outsourced operations. Juvenile Justice should evaluate SOC reports for all significant third-party service providers.

   Response
   DJJ has obtained the latest SOC report from our healthcare benefits program provider for direct-care youth (Anthem). We have implemented an annual review process which will be completed by the Bon Air Business Manager with assistance as needed from the IT Department. Evidence of the review and date of the review will be documented for auditing purposes.

10. Juvenile Justice did not properly identify and account for leases in accordance with the CAPP Manual and Governmental Accounting Standards Board (GASB) Statement No. 87. Juvenile Justice recorded leases they should not have, potentially causing duplicate lease information within the Commonwealth's Annual Comprehensive Financial Report. Juvenile Justice also did not properly evaluate and record the group of leased assets with the same contracted vendor, lease term, and interest rate. In addition, Juvenile Justice did not follow the correct procedure to determine the interest rate. CAPP Manual Topic 31200, which references GASB Statement No. 87, requires agencies to properly identify leases and group leases for recording in the lease accounting system to ensure proper classification of long-term and short-term, and to evaluate explicit, implicit, and incremental borrowing rates before defaulting to

the prime rate for a reasonable and accurate interest rate. Management should update lease processes and ensure it properly records and classifies leases.

Response
DJJ has reviewed its comprehensive lease listing to track all long-term and short-term leases. The accountant will review and evaluate leases quarterly, to determine if beneficial to group leases for purposes of disclosure. The first step in achieving this goal was to confirm leases with IT to ensure there is no potential duplication of leases held by other agencies and make necessary corrections. Management has begun updating the policies and processes to ensure that classification of all leases is identified and grouped properly. DJJ has begun to research methods in which to calculate the incremental borrowing rate for a reasonable and accurate rate.

11. Juvenile Justice's procedures on employee separations include a checklist to ensure the proper documentation for an employee that has separated from the agency. However, Juvenile Justice was unable to provide supporting documentation showing management completed this checklist for two out of four (50%) employees reviewed. Juvenile Justice should ensure it is completing the employee separations checklist and retaining this documentation for off-boarding employees.

Response
DJJ is in the final review of updating the agency's administrative procedure for separating employees from the department. This includes an updated and electronic version of an employee separation checklist, updated HR specific separation desk procedure, employee exit survey and shared notification of separating employees to all impacted divisions. Managers will be trained on the updated process. HR will ensure the notification to all impacted divisions is submitted. HR will follow the updated desk procedure to ensure receipt of the employee separation checklist and all supporting final documents to be maintained in the employee personnel file. The employee personnel file of the separated employee will be updated from active within the next pay period following separation. Managers who do not follow the updated procedures will be reported to the respective Deputy Director to address performance under DHRM Policy 1.60 Standards of Conduct and DHRM Policy 1.40. HR will conduct random audit checks quarterly on separated personnel files and we plan to have this process in place by May 1, 2024.

12. Juvenile Justice did not maintain documentation showing supervisors granted approval prior to employees working overtime. For one of four employees reviewed, there was no evidence that supervisors approved the overtime worked. Juvenile Justice should ensure that employees receive the proper approval for overtime prior to the employee working overtime and retain evidence of this approval.

Response
DJJ implemented use of [redacted] time and attendance timecards. All working hours, overtime, compensatory and personal leave must be keyed into [redacted] on the employee's timecard. Use of [redacted] permits HR to review timecards requiring management approval. All non-exempt employees follow the FLSA practice and law. Exempt employees who have been granted a blanket approval to work overtime due to the organizational strain is due to end. Effective April 1, 2024, all exempt employees must have a written approval from the Deputy Director or higher prior to working and receiving pay. HR will update the approved employee's [redacted] timecard to allow

for overtime to be recorded and approved. If no written approval is granted by the Deputy Director or higher, exempt employees will receive compensatory leave. The written approval must be submitted to HR and will be maintained electronically on HR secured drive.

We thank you for providing the opportunity for response and taking the time to consider our efforts to rectify the findings. We look to hearing from you with the final document and the process for moving forward.

Sincerely,

Amy M. Floriano