



DEPARTMENT OF CRIMINAL JUSTICE SERVICES

INTERNAL CONTROL QUESTIONNAIRE REVIEW RESULTS AS OF JUNE 2022

Auditor of Public Accounts
Staci A. Henshaw, CPA

www.apa.virginia.gov

(804) 225-3350



- TABLE OF CONTENTS -

	<u>Pages</u>
REVIEW LETTER	1-4
AGENCY RESPONSE	5-6



Commonwealth of Virginia

Auditor of Public Accounts

Staci A. Henshaw, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

October 10, 2022

Jackson Miller, Executive Director
Department of Criminal Justice Services
1100 Bank Street
Richmond, VA 23219

INTERNAL CONTROL QUESTIONNAIRE REVIEW RESULTS

We have reviewed the Internal Control Questionnaire for the **Department of Criminal Justice Services** (Criminal Justice). We completed the review on June 21, 2022. 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 Criminal 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 Criminal 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 all prior review findings, including findings in the report titled [Cycled Agency Information Systems Security Review for the year ended June 30, 2019](#). The agency has taken adequate corrective action with respect to all findings reported in the prior reviews from 2020 and 2019, respectively, 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 each agency. At some agencies only inquiry was necessary, while others included an in-depth analysis of the quality of the Stage 1 Agency-Level Internal Control Assessment Guide, or Stage 2 Process or Transaction-Level Control Assessment ARMICS processes. Our review of Criminal 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 Criminal 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, capital assets, grants management, 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:

- **Partial Repeat** – Criminal Justice continues to not have an adequate information technology (IT) security governance structure to manage its information security program and comply with the Commonwealth's Information Security Standard, SEC 501 (Security Standard). Specifically, Criminal Justice has control weaknesses in the following areas:
 - Criminal Justice does not have an established, documented, and implemented information security program that is sufficient to protect the agency's IT systems, as required in the Security Standard, Sections 1.4 and 2.4.2.

- Criminal Justice has not completed implementation of policies and procedures related to information security, as required in the Security Standard, Sections AU-1, CA-1, CM-1, CP-1, IA-1, IR-1, MA-1, PL-1, PS-1, RA-1, SA-1, SC-1, and SI-1.

Since the last review, Criminal Justice has hired a full time Information Security Officer that is responsible for creating an information security program. Criminal Justice should continue to develop and implement policies and procedures that are compliant with the requirements of the Security Standard.

- **Repeat** - Criminal Justice continues to not include all the components of its Disaster Recovery Plan (DRP) in its continuity planning documents and is not performing an annual exercise of the DRP components. The Security Standard, Section CP-1-COV-1, requires that agencies use their Business Impact Analysis and Risk Assessments to develop IT disaster components of the agency continuity plan which identify each IT system that is necessary to recover agency business functions or dependent business functions and requires an annual exercise of IT DRP components to assess their adequacy and effectiveness. Criminal Justice's Continuity of Operations Plan includes some of the required components but does not include all required components for each system. Criminal Justice should continue to develop a formal IT DRP document including all required elements and should perform annual testing of the IT DRP components.
- **Partial Repeat** - Criminal Justice continues to not have appropriate controls in place to ensure that access to their systems is appropriate and complies with the requirements of the Security Standard. While Criminal Justice recently approved an Access Control Policy, it has not yet implemented the requirements within that policy. Specifically, Criminal Justice has control weaknesses in the following areas:
 - Criminal Justice does not have an adequate process in place for reviewing and confirming ongoing operational need for current logical and physical access authorizations to information systems/facilities upon reassignment or transfer of employees to other positions within the organization, as required by the Security Standard, Section PS-5.
 - Criminal Justice does not have an adequate process in place for an annual review of systems access, as required by the Security Standard, Section AC-2.

Criminal Justice should continue to implement the controls outlined in its Access Control Policy to align with the Security Standard to ensure consistent and appropriate account management and to ensure the protection of sensitive, mission critical information.

- **Partial Repeat** - Criminal Justice continues to not document and implement system logging and monitoring procedures as required by the Security Standard. We identified two instances where Criminal Justice does not meet the minimum logging and monitoring requirements and communicated those to management in a separate document marked Freedom of Information Act Exempt under § 2.2-3705.2 of the Code of Virginia due to it containing descriptions of security mechanisms. Criminal Justice should implement the appropriate

logging and monitoring controls for its business environment to reduce the risk to data confidentiality, integrity, and availability.

- **Partial Repeat** – For some key business areas, Criminal Justice could not provide internal policies and procedures and some existing policies and procedures did not contain evidence of management’s review and approval. As Topic 20905 and other sections of the Commonwealth Accounting Policies and Procedures Manual require each agency to “publish its own policies and procedures documents, approved in writing by agency management,” Criminal Justice should draft and implement formalized policies and procedures over all key business areas and retain evidence of management’s approval over the policies.

We discussed these matters with management on July 21, 2022. 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.

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



COMMONWEALTH of VIRGINIA

Department of Criminal Justice Services

The Honorable Jackson H. Miller
Director

Tracy Louise Winn Banks, Esq.
Chief Deputy Director

Washington Building
1100 Bank Street
Richmond, Virginia 23219
(804) 786-4000
www.dcjs.virginia.gov

December 2, 2022

Ms. Staci A. Henshaw
Auditor of Public Accounts
Commonwealth of Virginia
P.O. Box 1295
Richmond, VA 23218

Dear Ms. Henshaw;

This is in response to the Internal Control Review conducted for the Virginia Department of Criminal Justice Services (DCJS), completed on June 21, 2022, and communicated to DCJS on October 10, 2022. There has been a delay in responding due to misdirection of email correspondence to DCJS.

The review results identified the following areas of improvement:

- **Partial Repeat** – Criminal Justice continues to not have an adequate information technology (IT) security governance structure to manage its information security program and comply with the Commonwealth's Information Security Standard, SEC 501 (Security Standard). Specifically, Criminal Justice has control weaknesses in the following areas:
 - Criminal Justice does not have an established, documented, and implemented information security program that is sufficient to protect the agency's IT systems, as required in the Security Standard, Sections 1.4 and 2.4.2.
 - Criminal Justice has not completed implementation of policies and procedures related to information security, as required in the Security Standard, Sections AU-1, CA-1, CM-1, CP-1, IA-1, IR-1, MA-1, PL-1, PS-1, RA-1, SA-1, SC-1, and SI-1.
 - Since the last review, Criminal Justice has hired a full time Information Security Officer that is responsible for creating an information security program. Criminal Justice should continue to develop and implement policies and procedures that are compliant with the requirements of the Security Standard.
- **Repeat** – Criminal Justice continues to not include all the components of its Disaster Recovery Plan (DRP) in its continuity planning documents and is not performing an annual exercise of the DRP components. The Security Standard, Section CP-1-COV-1, requires that agencies use their Business Impact Analysis and Risk Assessments to develop IT disaster components of the agency continuity plan which identify

each IT system that is necessary to recover agency business functions or dependent business functions and requires an annual exercise of IT DRP components to assess their adequacy and effectiveness. Criminal Justice's Continuity of Operations Plan includes some of the required components but does not include all required components for each system. Criminal Justice should continue to develop a formal IT DRP document including all required elements and should perform annual testing of the IT DRP components.

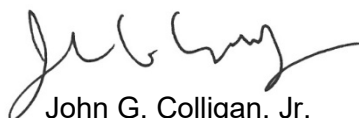
- **Partial Repeat** – Criminal Justice continues to not have appropriate controls in place to ensure that access to their systems is appropriate and complies with the requirements of the Security Standard. While Criminal Justice recently approved an Access Control Policy, it has not yet implemented the requirements within that policy. Specifically, Criminal Justice has control weaknesses in the following areas:
 - Criminal Justice does not have an adequate process in place for reviewing and confirming ongoing operational need for current logical and physical access authorizations to information systems/facilities upon reassignment or transfer of employees to other positions within the organization, as required by the Security Standard, Section PS-5.
 - Criminal Justice does not have an adequate process in place for an annual review of systems access, as required by the Security Standard, Section AC-2.

Criminal Justice should continue to implement the controls outlined in its Access Control Policy to align with the Security Standard to ensure consistent and appropriate account management and to ensure the protection of sensitive, mission critical information.

- **Partial Repeat** – Criminal Justice continues to not document and implement system logging and monitoring procedures as required by the Security Standard. We identified two instances where Criminal Justice does not meet the minimum logging and monitoring requirements and communicated those to management in a separate document marked Freedom of Information Act Exempt under § 2.2-3705.2 of the Code of Virginia due to it containing descriptions of security mechanisms. Criminal Justice should implement the appropriate logging and monitoring controls for its business environment to reduce the risk to data confidentiality, integrity, and availability.
- **Partial Repeat** – For some key business areas, Criminal Justice could not provide internal policies and procedures and some existing policies and procedures did not contain evidence of management's review and approval. As Topic 20905 and other sections of the Commonwealth Accounting Policies and Procedures Manual require each agency to "publish its own policies and procedures documents, approved in writing by agency management," Criminal Justice should draft and implement formalized policies and procedures over all key business areas and retain evidence of management's approval over the policies.

DCJS is in agreement with these findings and is currently working to eliminate them. Please contact me if you have any further questions.

Sincerely,



John G. Colligan, Jr.
Director of Finance and Administration