VIRGINIA

ALCOHOLIC BEVERAGE CONTROL

AUTHORITY

REPORT ON AUDIT

FOR YEAR ENDED

JUNE 30, 2022

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

AUDIT SUMMARY

We have audited the basic financial statements of the Virginia Alcoholic Beverage Control Authority (Authority) as of and for the year ended June 30, 2022, and issued our report thereon, dated November 17, 2022. Our report is included in the Authority's Annual Report that it anticipates releasing in December 2022.

Our audit of the Authority found:

- the financial statements are presented fairly, in all material respects;
- eight internal control findings requiring management's attention; however, we do not consider them to be material weaknesses; and
- four instances of noncompliance or other matters required to be reported under Government Auditing Standards.

The Authority has not taken adequate corrective action with respect to previously reported findings. Accordingly, we designated these findings with a "repeat" label in the section titled "Internal Control and Compliance Findings and Recommendations."

–TABLE OF CONTENTS–

	Pages
AUDIT SUMMARY	
INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS	1-7
INDEPENDENT AUDITOR'S REPORT ON INTERNAL CONTROL OVER FINANCIAL REPORTING AND ON COMPLIANCE AND OTHER MATTERS	8-10
AUTHORITY RESPONSE	11-14
AUTHORITY OFFICIALS	15

INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS

Continue Improving Database Security
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Yes (first issued in fiscal year 2019)

The Alcoholic Beverage Control Authority (Authority) continues to improve security for the database that supports its human resource system in accordance with the National Institute of Standards and Technology Standard, 800-53 (NIST Standard), and industry best practices. While the Authority has made limited progress since the prior year, five weaknesses remain.

We communicated the control weaknesses to management in a separate document marked Freedom of Information Act Exempt (FOIAE) under § 2.2-3705.2 of the Code of Virginia due to it containing descriptions of security mechanisms. The NIST Standard and industry best practices require the implementation of certain controls to reduce unnecessary risk to data confidentiality, integrity, and availability in systems processing or storing sensitive information. The weaknesses continue to exist due to limited staffing as well as the absence of some documented processes and consistent implementation of those processes.

The Authority should dedicate the necessary resources to ensure database configurations, controls, and processes align with the requirements in its policies, the NIST Standard, and industry best practices. This will help maintain the confidentiality, integrity, and availability of mission-critical data.

Continue Improving Security Awareness and Training Program
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Partial (first issued in fiscal year 2019)
Prior Title: Improve Security Awareness Training Program

The Authority continues to improve its information security awareness and training program to ensure all users complete training related to the Authority's policies for accessing its information systems and controls that protect the confidentiality, integrity, and availability of sensitive data.

Since the prior year audit, the Authority partially resolved one of the two weaknesses by revising its policies and procedures to define target completion rates for its Central Office, Enforcement and Retail employees based on organizational risk and user group. Defining the completion goals for the two employee groups with access to information systems allows the Authority to monitor training completion while also taking into consideration certain circumstances like staff turnover within the retail stores. Target completion rates also allow the Authority to determine whether management should take further enforcement measures for users to complete security awareness training to reduce risk to the Authority's sensitive information. However, the Authority continues to not define which training modules it requires each employee group to complete, or address whether its Warehouse employees,

who do not have access to information systems, must receive training as it relates to their roles and responsibilities on a time-specific basis.

The Authority's Security Awareness and Training Policy, which aligns with the NIST Standard, requires all users to complete security awareness training within 30 days of receiving access to the Authority's resources. Additionally, the policy requires users to annually attend security awareness refresher training and sign an acknowledgement stating they have read and understand the Authority's acceptable use policy. Furthermore, the Authority's Security Awareness and Training Policy requires the Authority to provide its staff sufficient training and supporting reference materials to allow them to protect the Authority's data and assets.

By not clearly defining its requirements for training assignments to specific employee groups, the Authority cannot ensure that each employee group is receiving the required training curriculum on a consistent basis. Also, without a consistent process to monitor and enforce users to complete security awareness and role-based training within the required timeframe, the Authority increases the risk that users will be more susceptible to malicious attempts to compromise physical access to sensitive data, such as ransomware, phishing, and social engineering. The Authority's Information Security Officer (ISO) left in December 2021, and the position remained vacant for six months until the Authority hired a new ISO in June 2022, which contributed to the delay of the Authority revising its policies and procedures and training curriculum.

The Authority should continue revising its policies and procedures to clearly document its requirements and process to assign training to specific employee groups. Additionally, the Authority should continue monitoring the employees' completion of training to determine whether it has met its target completion rates. If the Authority does not meet its target completion rates, the Authority should implement other enforcement measures for employees to complete training and reduce the risk to the Authority's sensitive information. The Authority should also continue improving its training curriculum for its Warehouse employees and implement a process for consistently administering this training. Improving and implementing the security awareness and training program will help protect the Authority from malicious attempts to compromise the confidentiality, integrity, and availability of sensitive data and assets. The Authority assigned the revised training to its Central Office and Retail employees at the end of June 2022 with a required completion date of December 2022. We will review the implementation of the revised training and target rates during our next audit.

Continue Improving Oversight of Third-Party Service Providers

Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Yes (first issued in 2020)
Prior Title: Improve Oversight of Third-Party Service Providers

The Authority continues to develop a formal and consistent process to oversee and manage its third-party service providers in accordance with the NIST Standard. Due to the departure of the ISO in December 2021, the Authority was unable to perform corrective actions during fiscal year 2022 to resolve the prior year's three weaknesses. However, the new ISO, hired in June 2022, has begun drafting

a new policy and process for managing third-party providers with an expected implementation during 2023.

The NIST Standard requires the Authority to employ methods to monitor security control compliance by the providers on an ongoing basis. Without a formal and consistent process to gain assurance that its providers implement information security controls, and that they operate effectively, the Authority cannot guarantee its data is secure in accordance with its policies and the NIST Standard.

The Authority should continue developing and implementing formal policies and procedures to oversee and manage its third-party service providers and address the three weaknesses in the prior report. Additionally, the Authority should enforce its new process to ensure consistent oversight of providers. This will ensure the providers adhere to the same security controls that govern the Authority's internal information technology systems and confirm overall compliance with the requirements outlined in the NIST Standard.

Continue Improving Internal Controls over Employment Eligibility
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Yes (first issued in 2021)
Prior Title: Improve Internal Controls over Employment Eligibility Process

The Authority's Human Resources department has not completed Employment Eligibility Verification (I-9) forms in accordance with guidance issued by the U.S. Citizenship and Immigration Services of the U.S. Department of Homeland Security. Our sample of 25 employees hired by the Authority during fiscal year 2022 found:

- Human Resources did not use the correct I-9 Form for one of 25 employees (4%).
- Three of 25 employees (12%) did not sign Section 1 of the form by the first day of employment.
- Human Resources did not complete Section 2 properly for one of 25 employees (4%).
- Human Resources did not complete Section 2 of the I-9 form timely for two of 25 employees (8%).
- Human Resources did not create a case in the E-Verify system within three days of the first day of employment for nine of 25 employees (36%).
- Human Resources did not complete a case in the E-Verify system for one of 25 employees (4%).

Failure to correctly and timely complete I-9 forms can result in penalties. Additionally, § 40.1-11.2 of the Code of Virginia requires the use of the E-Verify system. The Human Resources Director should ensure that Human Resources staff receive proper training on the U.S. Department of Homeland Security's guidelines and use of the E-Verify system. Internal policies should clearly address use of the E-Verify system and the Human Resources Director should ensure that staff follow those guidelines.

Continue Improving Internal Controls over Processing Payments
Type: Internal Control
Severity: Significant Deficiency
Repeat: Partial (first issued in fiscal year 2021)
Prior Title: Improve Internal Controls Over Processing Payments

The Authority did not process payments in compliance with the Authority's Signature Authority & Procurement Responsibility policy. During fiscal year 2022, the Authority processed approximately 18,000 payments. Over 9,000 of these payments are related to the purchase of spirits through the bailment inventory process, distillery payments, or rent payments. Since the Authority's inventory system internally generates the bailment statements, and distillery and rent payments do not follow the standard accounts payable process, we excluded these payments from our review of vendor invoices.

In our sample of 30 payments, for which prompt payment requirements were applicable, we identified six instances in which the Authority did not process payment within the required 30 days. In addition, we identified four instances in which dates on supporting documentation did not match dates entered in the system. Per the Authority's policy, Accounts Payable establishes the required payment due date based on the terms of the contract; or if a contract is not in existence, 30 calendar days after the receipt of a proper invoice, or 30 days after the receipt of goods or services, whichever is later. By not ensuring timely payments, the Authority may harm their reputation as a buyer, damage relationships with vendors, and could incur late fees.

Late payments were primarily the result of individuals responsible for receiving goods and services not performing their duties timely. Accounts Payable's process requires a three-way match before processing payment; therefore, Accounts Payable cannot process payments for respective vendor charges until the receiver marks the purchase as received in the Commonwealth's procurement system.

Accounts Payable identified a category of utility bills which historically had a higher risk of late payments. The Authority implemented a new process related to these utility bills in March 2022, which has improved the timeliness of payments. The Authority should continue to improve processes to ensure that departments mark items as received within the Commonwealth's procurement system and submit required documentation in a timely manner to Accounts Payable to ensure the Authority makes all payments within the 30-day period. Additionally, the Authority should ensure staff enters accurate dates into the Commonwealth's procurement system, so that the Authority can properly monitor adherence to its policy.

Improve Internal Controls over Employee Separation Process

Type: Internal Control
Severity: Significant Deficiency
Repeat: No

The Authority does not have adequate internal controls over the completion of off-boarding checklists or removing access for terminated employees. Our sample of 27 terminated employees during fiscal year 2022 found:

- Two of 27 (7%) separation checklists remained incomplete 80 and 117 business days after the employees' termination date.
- Supervisors completed ten of 27 (37%) checklists six to 90 business days after the employees' termination date.
- For 10 of 27 (37%) employees, the Authority removed system access seven to 66 business days after the employees' termination date. Two instances were related to the Authority's active directory and eight instances were related to the Commonwealth's electronic procurement system.
- Seventeen of 27 (63%) of the dates on the checklist did not agree to the date the Authority removed the employee's system access.

The Authority's human resource system generates an off-boarding checklist with multiple sections for completion by various departments. The five-day timeframe within the separation procedure is specific only to the section of the checklist the direct supervisor must complete. The policy does not define specific timeframes for the completion of other sections, which includes human resources, payroll, and information systems, nor does it define a timeframe for system removal. This makes it difficult to enforce adherence to policy and ensure timeliness of completion. Additionally, Human Resources has not updated the separation checklist to reflect changes in systems (system retirements and new system implementations) to ensure system access is properly removed.

The Authority relies on active directory system access removal for removal of access to many of the Authority's critical systems, including the financial management system and the inventory and logistics system. Therefore, Human Resources does not track the removal of system access outside of the Authority's active directory. This leaves systems outside of the Authority's active directory, such as the Commonwealth's statewide systems, at risk for the Authority not removing access timely.

A critical function of completed checklists is to ensure the timely removal of access to the Authority's systems and return of property. The Authority should review their current termination practices to ensure their policy is reasonable and effective internal controls are in place. Additionally, due to their unique structure, the Authority should define specific procedures for retail store employees, enforcement employees, and headquarter employees as access levels and risks are inherently different. This will enable Human Resources to better monitor and hold supervisors accountable for timely completion of the employee checklist and access removal.

Implement a Data/Records Retention Policy and Solution for Automated Reconciliations

Type: Internal Control
Severity: Significant Deficiency
Repeat: No

The Authority's information system environment includes various systems which periodically interface with each other. The Authority relies on automated system reconciliations to ensure the data interface between various systems is complete and accurate. During fiscal year 2022, the Authority did not retain complete documentation for the following automated reconciliations:

- Point of Sale System to the Customer Activity Repository
- Licensing and Fees System to the Customer Activity Repository
- Customer Activity Repository to the Financial Management System

The Authority's newly implemented Customer Activity Repository only retains reconciliation reports for 90 days. As a result, we were unable to review reconciliation reports for the first three quarters of fiscal year 2022. The Commonwealth's Accounting Policies and Procedures Manual (CAPP Manual) Section 20900 – Reconciliation Procedures, prescribes the level of detail at which agencies must reconcile records, accounts, and logs depending on the nature of the transactions. If recorded in multiple systems, transactions should be traceable from one system to another, any variance between accounting data should be traceable to specific transactions, and agencies should explain and justify all variances. Additionally, agencies should maintain documentation that enables accountants to follow an audit trail through the accounting process from each transaction to appropriate reports and other output. Although the Authority is exempt from CAPP Manual requirements, we feel these requirements are an appropriate basis for industry best practices.

By not retaining documentation and support for automated reconciliations, the Authority may have difficulty investigating discrepancies between systems, and may be unable to show that two systems reconciled as of a specific date. The Authority should implement a process to ensure the various systems retain all automated reconciliation reports. Additionally, the Authority should consider implementing a control to log when employees review the automated reconciliation reports in accordance with Authority's policies and procedures.

Retain Inventory Documentation
Type: Internal Control
Severity: Significant Deficiency
Repeat: No

The Authority conducts inventory counts at all retail stores and makes necessary adjustments in the inventory system to ensure the quantities in the system are complete and accurate. During fiscal year 2022, the Authority did not retain records of the actual counts for the retail store inventories. Due to system limitations, the Authority only retains the electronic data generated from the counts for 60 days. As a result of not retaining the inventory count data, we were unable to review support for the manual adjustments in the inventory system resulting from the inventory counts.

CAPP Manual Section 21000 – Records Retention/Disposition, requires agencies to preserve and maintain records such that they are accessible throughout their lifecycle. Although the Authority is exempt from CAPP Manual requirements, we feel these requirements are an appropriate basis for industry best practices. The Authority should retain documentation and support for all inventory adjustments, including the electronic records of each inventory count. This will help establish an audit trail and reduce the risk of errors in the manual adjustment process. The documentation for each inventory adjustment should include the quantity counted, the employee who conducted the count, and management review. Without inventory count documentation, the Authority may have difficultly investigating discrepancies and ensuring that complete inventories occur. The Authority should establish a new data retention process for inventory counts and update the inventory policy to address the retention of inventory documentation.

Commonwealth of Virginia

Auditor of Public Accounts

Staci A. Henshaw, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

November 17, 2022

The Honorable Glenn Youngkin
Governor of Virginia

Joint Legislative Audit
and Review Commission

Alcoholic Beverage Control Board
Virginia Alcoholic Beverage Control Authority

INDEPENDENT AUDITOR'S REPORT ON INTERNAL CONTROL OVER FINANCIAL REPORTING AND ON COMPLIANCE AND OTHER MATTERS

We have audited, in accordance with the auditing standards generally accepted in the United States of America and the standards applicable to financial audits contained in Government Auditing Standards, issued by the Comptroller General of the United States, the financial statements of the **Virginia Alcoholic Beverage Control Authority** (Authority) as of and for the year ended June 30, 2022, and the related notes to the financial statements, which collectively comprise the Authority's basic financial statements, and have issued our report thereon dated November 17, 2022.

Internal Control Over Financial Reporting

In planning and performing our audit of the financial statements, we considered the Authority's internal control over financial reporting (internal control) as a basis for designing audit procedures that are appropriate in the circumstances for the purpose of expressing our opinion on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of the Authority's internal control. Accordingly, we do not express an opinion on the effectiveness of the Authority's internal control.

A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, misstatements on a timely basis. A material weakness is a deficiency, or a combination of deficiencies, in internal control, such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected, on a timely basis. A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance.

Our consideration of internal control was for the limited purpose described in the first paragraph of this section and was not designed to identify all deficiencies in internal control that might be material weaknesses or significant deficiencies and, therefore, material weaknesses or significant deficiencies may exist that were not identified. Given these limitations, during our audit we did not identify any deficiencies in internal control that we consider to be material weaknesses. We did identify certain deficiencies in internal control titled "Continue Improving Database Security," "Continue Improving Security Awareness and Training Program," "Continue Improving Oversight of Third-Party Service Providers," "Continue Improving Internal Controls over Employment Eligibility Process," "Continue Improving Internal Controls over Processing Payments," "Improve Internal Controls over Employee Separation Process," "Implement a Data/Records Retention Policy and Solution for Automated Reconciliations," and "Retain Inventory Documentation," which are described in the section titled "Internal Control and Compliance Findings and Recommendations," that we consider to be significant deficiencies.

Compliance and Other Matters

As part of obtaining reasonable assurance about whether the Authority's financial statements are free of material misstatement, we performed tests of its compliance with certain provisions of laws, regulations, contracts, and grant agreements, noncompliance with which could have a direct and material effect on the financial statements. However, providing an opinion on compliance with those provisions was not an objective of our audit and**,** accordingly, we do not express such an opinion. The results of our tests disclosed instances of noncompliance or other matters that is required to be reported under Government Auditing Standards and which are described in the section titled "Internal Control and Compliance Findings and Recommendations" in the findings titled "Continue Improving Database Security," "Continue Improving Security Awareness and Training Program," "Continue Improving Oversight of Third-Party Service Providers" and "Continue Improving Internal Controls over Employment Eligibility."

The Authority's Response to Findings

We discussed this report with management at an exit conference held on November 18, 2022. Government Auditing Standards require the auditor to perform limited procedures on the Authority's response to the findings identified in our audit and described in the accompanying section titled "Authority Response." The Authority's response was not subjected to the other auditing procedures applied in the audit of the financial statements and, accordingly, we express no opinion on the response.

Status of Prior Findings

The Authority has not taken adequate corrective action with respect to the previously reported findings "Continue Improving Database Security," "Improve Security Awareness Training Program," "Improve Oversight of Third-Party Service Providers," "Improve Internal Controls over Employment Eligibility Process," and "Continue Improving Internal Controls over Processing Payments." Accordingly, we included these findings in the section entitled "Internal Control and Compliance Findings and Recommendations."

Purpose of this Report

The purpose of this report is solely to describe the scope of our testing of internal control and compliance and the results of that testing, and not to provide an opinion on the effectiveness of the entity's internal control or on compliance. This report is an integral part of an audit performed in accordance with Government Auditing Standards in considering the entity's internal control and compliance. Accordingly, this communication is not suitable for any other purpose.

Staci A. Henshaw
AUDITOR OF PUBLIC ACCOUNTS

JMR/vks

November 17, 2022

Ms. Staci A. Henshaw, CPA
Auditor of Public Accounts
101 N. 14th Street
Richmond, VA 23219

Dear Ms. Henshaw,

Attached are the Virginia Alcohol Beverage Control Authority ("VA ABC," the "Authority") responses to the audit for fiscal year ended June 30, 2022. The Authority appreciates the opportunity to respond to the findings noted, and to strengthen our controls based on the recommendations. Our responses to the findings in the Report on Internal Controls follow.

Continue Improving Database Security

The Authority agrees that it will dedicate the necessary resources to continue to make progress ensuring database configurations, controls, and processes align with the requirements in its policies, the National Institute of Standards and Technology (NIST), and industry best practices. The Authority's investments continue to make progress in maintaining the confidentiality, integrity, and availability of mission critical data. As VA ABC retires legacy systems, we will continue to assess internal controls to make improvements and progress.

Improve Security Awareness Training Program

The Authority agrees that its security awareness training program (SAT) was only partially implemented during the fiscal year in audit. The Authority has since fully implemented the program, including adding the target group completion rate by specific defined groups within its policy. During the last two calendar years we developed our own training modules, including role-based training, and are refining our process for deployment and monitoring of the training modules. The Authority also added the Distribution Center employees to its SAT scope, which had previously been excluded in the SAT program. We continue to look for ways to improve the monitoring and reporting process. VA ABC's policy does allow for enforcement measures to ensure users complete required training, although VA ABC uses these as a last resort.

Improve Oversight of Third-Party Service Providers

The Authority agrees with the finding and will develop an IT Third Party Management Policy to include requirements for IT Security considerations. The Information Security Officer (ISO) will work with the Chief Information Officer (CIO) and with the Procurement division to define and identify the requirements for IT vendor risk and control Reporting reviews. The Authority will incorporate the IT Security requirements into the contract process review for new contracts, which will include documenting associated risks resulting from decisions to remove security requirements.

The Authority will work with Procurement to identify the current inventory of service providers and develop an IT risk review schedule. Information Security & Governance will review the current process with procurement to address the completion of provider IT risk reviews and will develop a process that is sustainable and includes ongoing monitoring and compliance.

Improve Internal Controls over Employment Eligibility Process

The Authority concurs with the exceptions noted and will enhance controls over completion and review of Employment Eligibility Verification (I-9) forms, to ensure compliance with guidance issued by the U.S. Citizenship and Immigration Services of the U.S. Department of Homeland Security. HR will create a daily I-9 control checklist report that will include all the required and appropriate information to assist in determining if an employee's I-9 is completed in accordance with Federal regulations. HR will ensure increased compliance as well as provide additional training for our Retail Hiring managers on the accurate completion and timely submission of the I-9 documents and will conduct weekly I-9 and e-verify audits to ensure increased compliance. Lastly, we will review all policies and divisional standard operating

procedures to ensure they clearly address the use of the e-verify system, and we will re-educate the HR team on compliance obligations related to the U.S. Department of Homeland Security's guidelines and use of the e-verify system.

Improve Internal Controls Over Processing Payments

The Authority concurs that the Authority did not process payments on the exceptions noted by APA on vendor-initiated invoices which excludes payments for spirits and mixers, distillery payments and rent payments, within the required 30 days. The Division of Financial Management Services' Accounts Payable (AP) department will retrain and continue to reinforce, amongst the Authority's designated department receivers, the importance of confirming and approving receipt of goods and services in a timely manner to ensure that the Authority can make all payments within the 30-day period. Accounts Payable's Assistant Manager will continue to monitor and report payment delays by sending out weekly reminders to receivers, with a copy of the reminder to their respective supervisors on the third notification. Expenses that are not approved and submitted by receivers in the Commonwealth's Procurement System by the third reminder, will be escalated to the Assistant Controller and Director of Finance. Lastly, the AP department will update their review process to ensure that accounts payable analysts are reviewing accuracy of dates input by designated receivers into the Commonwealth's Procurement System, so that the Authority can properly monitor adherence to policy.

Improve Internal Controls over Employee Separation Process

The Authority concurs with the exceptions noted and will enhance controls over employee separation process. The Authority will reassess our current processes and ensure all responsible leaders are following the guidelines related to the separation checklist. Furthermore, the Authority will provide additional training and support to the responsible leaders and will conduct quarterly audits to ensure compliance.

Implement a Data/Records Retention Policy and Solution

The Authority concurs with the exceptions noted and will improve its process to ensure that the various systems retain all automated reconciliation reports, and that applicable records are available for review in a clear and concise manner. Additionally, the Authority will implement a control to log when employees review the automated reconciliation reports in accordance with Authority's policies and procedures.

Retain Inventory Documentation

The Authority concurs with the exceptions noted and will retain documentation for inventory adjustments, including the electronic records of inventory counts to support proper audit trail and reduce the risk of errors in the manual adjustment process. Retail division will work with the Information Technology division to establish a new data retention process to support the documentation of each inventory adjustment including the quantity counted, the employee who conducted the count, and management review.

The Authority relies on its automated system when performing inventory counts and believes features of the system sufficiently enables the Authority to investigate discrepancies. The Authority also believes that it has sufficient oversight review to ensure that complete and proper inventory counts are conducted by the stores and that sufficient mitigating controls exist to ensure an accurate count of its inventory.

Sincerely,

Travis G. Hill
Chief Executive Officer

VIRGINIA ALCOHOLIC BEVERAGE CONTROL AUTHORITY

As of June 30, 2022

BOARD OF DIRECTORS

Maria J. K. Everett
Chair

Beth Hungate-Noland
Vice Chair

Gregory F. Holland
Member

Mark Rubin
Member

William “Bill” Euille
Member

OFFICIALS

Travis Hill
Chief Executive Officer

Jerome Fowlkes
Chief Administrative Officer

Eddie Wirt
Chief Communications and Research Officer

Thomas Kirby
Chief Bureau of Law Enforcement

John Daniel
Chief Government Affairs Officer and General Counsel

Paul Williams
Chief Information Officer

Mark Dunham
Chief Retail Operating Officer

Elizabeth Chu
Chief Transformation Officer