An Audit Report on

The Behavioral Health Executive Council

- The Council did not establish processes to verify National Practitioner Data Bank checks before issuing license renewals and license upgrades or perform fingerprint criminal history checks before issuing license upgrades.
- The Council did not properly control access to its network and regulatory system based on business needs.
- The Council had adequate controls for processing license applications and investigating complaints.

Lisa R. Collier, CPA, CFE, CIDA
State Auditor

The Behavioral Health Executive Council (Council) established processes and related controls to ensure that it complied with requirements related to processing expired and denied license applications; reviewing, investigating, and resolving complaints; and making the disciplinary information of licensees available to the public. However, the Council should implement controls to ensure that it checks the National Practitioner Data Bank before issuing license renewals and license upgrades and that it checks Federal Bureau of Investigation fingerprint criminal history records before issuing license upgrades.

This audit was conducted in accordance with Texas Government Code, Sections 321.013 and 321.0132.

Additionally, the logical access controls for the Council's information technology (IT) systems had significant weaknesses. The Council also did not establish certain application controls in its regulatory tracking system, VERSA Regulation, to ensure the integrity of its data, and it did not have policies and procedures for its IT functions.

HIGH

NEW LICENSES AND LICENSE RENEWALS

The Council did not verify National Practitioner Data Bank checks for license renewals and license upgrades or review fingerprint criminal history checks for license upgrades.

Chapter 1-A | p. 5

LOW

EXPIRED AND DENIED LICENSE APPLICATIONS

The Council complied with requirements for processing expired and denied license applications.

Chapter 1-B | p. 9

For more information about this audit, contact Audit Manager Cesar Saldivar or State Auditor Lisa Collier at 512-936-9500.

October 2023 | Report No. **24-002**

LOW

ENFORCEMENT

The Council had adequate controls to investigate and process complaints and make disciplinary actions publicly available in accordance with requirements.

Chapter 2 | p. 10

HIGH

INFORMATION TECHNOLOGY

The Council did not appropriately restrict access to its network and regulatory system.

Chapter 3 | p. 12

Summary of Management's Response

Auditors made recommendations to address the issues identified during this audit, provided at the end of certain chapters in this report. The Council agreed with all of the findings and most of the recommendations; the Council said it would accept the risk of not implementing one recommendation, related to segregation of duties, due to a limited number of staff.

Ratings Definitions

Auditors used professional judgment and rated the audit findings identified in this report. The issue ratings identified for each chapter were determined based on the degree of risk or effect of the findings in relation to the audit objective(s).

PRIORITY: Issues identified present risks or effects that if not addressed could ***critically affect*** the audited entity's ability to effectively administer the program(s)/function(s) audited. Immediate action is required to address the noted concern(s) and reduce risks to the audited entity.

HIGH: Issues identified present risks or effects that if not addressed could ***substantially affect*** the audited entity's ability to effectively administer the program(s)/function(s) audited. Prompt action is essential to address the noted concern(s) and reduce risks to the audited entity.

MEDIUM: Issues identified present risks or effects that if not addressed could ***moderately affect*** the audited entity's ability to effectively administer the program(s)/function(s) audited. Action is needed to address the noted concern(s) and reduce risks to a more desirable level.

LOW: The audit identified strengths that support the audited entity's ability to administer the program(s)/function(s) audited or the issues identified do not present significant risks ***or*** effects that would negatively affect the audited entity's ability to effectively administer the program(s)/function(s) audited.

For more on the methodology for issue ratings, see Report Ratings in Appendix 1.

Background Information

The Council consists of four member boards that regulate behavioral health services and social work.

The Behavioral Health Executive Council (Council) was created by the 86th Legislature in 2019. (See text box for a description of the Council's mission.) The Council's four member boards consist of the Texas State Board of Examiners of Psychologists and three boards previously overseen by the Health and Human Services Commission: the Texas State Board of Examiners of Marriage and Family Therapists, the Texas State Board of Examiners of Professional Counselors, and the Texas State Board of Social Worker Examiners.

License Types. Through its four member boards, the Council regulates the following professions:

- Licensed Specialist in School Psychology (LSSP).
- Licensed Psychological Associate (LPA).
- Licensed Psychologist (LP).
- Licensed Professional Counselor Associate (LPCA).
- Licensed Professional Counselor (LPC).
- Licensed Marriage and Family Therapist Associate (LMFTA).
- Licensed Marriage and Family Therapist (LMFT).
- Licensed Baccalaureate Social Worker (LBSW).
- Licensed Master Social Worker (LMSW).
- Licensed Clinical Social Worker (LCSW).

The Council's Mission

The mission of the Council is to protect and promote the welfare of the people of Texas by ensuring that behavioral health services and social work practice are provided by qualified and competent practitioners who adhere to established professional standards. This mission is derived from the duly enacted statutes governing each regulated profession, as well as the law creating the Council, and supersedes the interest of any individual or special interest group.

Source: The Council.

HIGH

Chapter 1-A
New Licenses and License Renewals

The Behavioral Health Executive Council (Council) should implement controls to ensure that it checks the National Practitioner Data Bank (NPDB) for license renewals and license upgrades (see text box for more on the NPDB's role) and that it checks Federal Bureau of Investigation (FBI) fingerprint criminal history records for license upgrades.

The Council did not verify National Practitioner Data Bank checks for license renewals and license upgrades as required.

None (0 percent) of the 30 license renewals tested had NPDB checks submitted as required by Texas Occupations Code, Section 507.258. The Council stated that it did not establish a process to verify NPDB checks for license renewals due to not having enough staff to conduct the checks and still review renewals in a timely manner. Delays in reviewing renewals cause licenses to become delinquent.

The Council verified NPDB checks for all (100 percent) of the 19 new licenses tested. However, the Council did not verify NPDB checks for 9 (90 percent) of 10 upgraded licenses tested. A license upgrade takes place when, for example, a Licensed Professional Counselor Associate becomes a Licensed Professional Counselor. The Council did not have a process to verify NPDB checks for license upgrades.

National Practitioner Data Bank

The National Practitioner Data Bank (NPDB) is a web-based repository of reports containing information on medical malpractice payments and certain adverse actions related to health care practitioners, providers, and suppliers. Established by Congress in 1986, it is a workforce tool that prevents practitioners from moving state to state without disclosure or discovery of previous damaging performance.

Source: The National Practitioner Data Bank.

While Texas Occupations Code, Section 507.258, does not require NPDB checks for license upgrades, not checking applicants' history in the NPDB increases the risk that the Council could issue,

upgrade, or renew licenses for applicants with a recorded history of disciplinary or other legal actions. Some associate licensees did not receive NPDB checks prior to the creation of the Council. In addition, some associate licensees are not required to upgrade to full licenses for five years after the issuance of initial licenses, and then do not renew for two additional years, which increases the length of time that licensees may go without NPDB checks.

The Council did not appropriately review fingerprint criminal history checks for new licenses.

Five (17 percent) of 29 new licenses tested did not have FBI fingerprint criminal history checks performed prior to license issuance as required by Texas Occupations Code, Section 507.251. The five new licenses without FBI fingerprint criminal history checks consisted of four license upgrades and one new license issued to an applicant with a license from out of state. The Council did not have a process to verify FBI fingerprint criminal history checks for license upgrades. The Council stated that the FBI fingerprint criminal history check for the applicant with a license from out of state was not performed due to oversight caused during the transition of licensing administration from the Health and Human Services Commission to the Council.

Not conducting FBI fingerprint criminal history checks increases the risk of issuing licenses to candidates who might be disqualified.

Recommendations

The Council should establish processes to:

- Verify NPDB checks for license applicants before issuing license renewals and license upgrades.
- Ensure that FBI fingerprint criminal history checks are performed for all issuances, upgrades, and renewals of licenses.

Management's Response

NPDB Concern, Ch. 1-A: The Council did not verify National Practitioner Data Bank checks for license renewals and licensed upgrades as required.

Management Response: Management agrees with the recommendations and will recommend to the Council that it make the necessary changes to 22 TAC 883.1 and begin requiring those licensees selected for an audit under 22 TAC 882.50, to submit a self-query report from the National Practitioner Data Bank (NPDB) as a condition of renewal.[1] While the optimal solution would be to subscribe to a continuous query from the NPDB on every licensee, or alternatively, require every renewing licensee to submit a self-query report as a condition of renewal, neither are practical (or achievable) solutions in terms of costs and staffing. The subscription costs for continuous queries on the Council's 80,000+ licensees would exceed $200,000 per year, and the Council simply does not have the staff needed to review self-query reports from every licensee renewing his or her license.

However, when combined with the mandatory reporting required by 22 TAC 884.32 and the Council's enforcement powers, management believes the aforementioned solution represents a reasonable approach to ensuring the public is protected from bad actors. This belief is further bolstered by the fact that very few complaints or investigations originate from third-party disciplinary databases such as the NPDB and ASPPB's Disciplinary Data System.

Additionally, the Council will begin requiring a self-query report be submitted from the National Practitioner Data Bank (NPDB) in connection with upgrade applications. While Section 507.258 of the Occupations Code only requires NPDB checks for initial and renewal applications, management understands the SAO's concerns and will begin requiring NPDB checks for upgrade applications as well.

[1] In the unlikely event the Council does not make the necessary rule changes to carry out this recommendation, management will request additional funding in the Council's 2025-26 LAR to cover the costs associated with subscribing to continuous queries for all licensees.

The staff primarily responsible for implementation are the Executive Director, General Counsel, and CFO. The estimated timeline for completion is 9 months.

Fingerprint Background Check Concern, Ch. 1-A: The Council did not appropriately review fingerprint criminal history checks for new licenses.

Management Response: Prior to the passage of HB1501 by the 86th Legislature, the MFT, LPC, and Social Work programs did not have authority to conduct fingerprint background checks. As a result, no such checks were conducted on applicants while these programs were administratively attached to HHSC. This created a scenario whereby applicants and LPC and MFT associate license holders transferred into the Council's database without having undergone a fingerprint background check.

With that understanding, management agrees with the recommendations and will identify those individuals who applied for or were licensed as LPC or MFT associates under HHSC without a fingerprint background check and subsequently came under the Council's jurisdiction. The Council will then require these individuals to undergo a fingerprint background check pursuant to 22 TAC 882.40. While the target population is relatively small, and despite the fact that this concern will ultimately resolve itself through the expiration of the associate license or the standard renewal process, the Council understands the SAO's concerns and will expedite the resolution by using its authority under 882.40.

The staff member primarily responsible for implementation is the Executive Director. The estimated timeline for completion is 6 months.

Chapter 1-B

LOW

Expired and Denied License Applications

The Council established processes to comply with requirements for processing expired and denied license applications.

The Council appropriately noted deficiencies in expired and denied license applications. It processed applications in compliance with applicable requirements, which include giving applicants an opportunity to resolve deficiencies. For denied applications, the Council provided 30 days for further review by member boards, as required. All denied applications were processed timely in accordance with Council rules.

LOW

Chapter 2
Enforcement

The Council had adequate controls to investigate and process complaints and make disciplinary actions publicly available in accordance with requirements.

The Council appropriately investigated and documented complaints it received.

When the Council receives a complaint, it determines whether or not there is probable cause to believe a violation has occurred. The Council investigated and processed all 30 probable cause complaints tested and 29 (97 percent) of 30 non-probable cause complaints tested as required. Its determinations of whether or not there was probable cause were supported. (See text box for the Council's definition of probable cause).

Probable Cause

Probable cause means the facts and circumstances within the agency's knowledge, and of which it has reasonably trustworthy information, are sufficient to warrant a prudent person in believing that the respondent committed a violation of the Council's rules or other law within the jurisdiction of the agency.

Source: The Council.

In addition, the Council appropriately documented reviews for 26 (87 percent) of 30 probable cause complaints and 29 (97 percent) of 30 non-probable cause complaints.

The Council assigned disciplinary actions resulting from all 13 applicable probable cause complaints tested according to its and its member boards' schedules of sanctions, and it monitored compliance with disciplinary orders according to its rules, including collecting the appropriate amounts for administrative penalty fees for all 10 applicable probable cause complaints tested.

The Council established adequate processes to make licensee disciplinary actions publicly available.

The Council established a process to make licensee disciplinary actions and eligibility orders available to the public, and 24 (96 percent) of 25 complaints resulting in disciplinary actions tested could be viewed via the Council's online license search.

An additional 11 (85 percent) of 13 complaints selected as part of probable cause complaint testing resulted in disciplinary actions that were also made available to the public.

HIGH

Chapter 3
Information Technology

The logical access controls for the Council's information technology (IT) systems had significant weaknesses. Additionally, the Council did not establish certain application controls in its regulatory tracking system, VERSA Regulation (VERSA), to ensure the integrity of its data, and it did not have policies and procedures for its IT functions.

The Council did not appropriately restrict access to its network and regulatory system.

Access Removal. The Council did not appropriately remove access to its network for 9 (13 percent) of 69 user accounts tested. Specifically:

- The Council did not immediately remove network access for one former employee who was terminated for cause. The account remained in the network for at least 231 days.
- The Council did not immediately remove network access for another former employee, a former contractor, and a person who was offered a position with the Council but did not show up as scheduled.
- The Council provided access to a user who works under the direction of the Health Professions Council (HPC), which provides IT support to the Council, but is employed at an unrelated regulatory agency. However, at the time of the audit, the Council and HPC did not have an agreement in place allowing for non-HPC employees to provide IT support to the Council.
- Four user accounts were disabled in the Council's active directory, but the Council was unable to provide documentation detailing the dates of those deactivations.

In addition, the Council did not appropriately restrict access to VERSA to ensure that only current employees or authorized contractors could access the system. Specifically, 3 (5 percent) of 62 users tested were not current employees. One of the three users also had active access to the Council's network, which is required for access to VERSA, at the time of the audit. Auditors verified that this user did not access VERSA after separation from the Council.

Access Assignment. The Council did not appropriately restrict access to the Uniform Statewide Accounting System (USAS) and VERSA to ensure that access was based on valid business needs. Specifically:

- Nine (15 percent) of 62 users tested did not have a business need for certain permissions in VERSA.
- Two USAS users were able to both enter and release (or post) transactions in USAS. During the audit scope, two transactions totaling $134 were either entered or modified and released by the same user.

Weaknesses in logical access controls increase the risk of unauthorized data manipulation and accidental or intentional sharing of potentially confidential data with unauthorized parties. Additionally, lack of segregation of duties may increase the risk of fraud and transaction errors.

The Council should strengthen controls for its regulatory tracking system.

The Council did not establish certain application input and processing controls in VERSA to ensure the integrity of its data. Of 23 fields tested, 5 (22 percent) did not have sufficient controls to ensure the integrity of licensing and/or enforcement data. Specifically:

- VERSA will accept an address entry for a license application that does not include a city or a zip code.
- VERSA allows a user to process a new complaint without entering a priority level, classification, or summary.

Lack of application controls increases the risks of inaccurate and incomplete data being entered for license applicants and delays in addressing critical complaints.

The Council did not properly establish policies and procedures for its IT functions.

The Council did not have documented policies and procedures to ensure that its IT systems are managed effectively and that its data is reliable and accurate.

Texas Administrative Code, Title 1, Section 202.21, requires each state agency to develop, document, and implement information security policies and procedures. Having documented policies and procedures would help ensure that only users with valid business needs had access to the Council's IT systems and help protect the integrity of the Council's data.

Recommendations

The Council should:

- Develop, document, and implement IT policies and procedures.
- Periodically review access to its IT systems to ensure that access is assigned according to valid business needs.
- Enforce proper segregation of duties for USAS and VERSA.
- Implement controls to ensure that data in VERSA is accurate and complete.

Management's Response

> **Network and Regulatory System Access, Ch. 3:** The Council did not appropriately restrict access to its network and regulatory system.
>
> **Management Response:** Management agrees with most of the recommendations regarding this concern and has already taken the corrective action necessary to address most of the concerns. More specifically, the Council has implemented a checklist system to ensure employees are granted network and system access based only upon their needs, and that former employees have their network and system access removed at the time of separation. Additionally, the

Council will develop a policy to ensure employee access to the network and system is reviewed on an appropriate, reoccurring basis. Lastly, the Council executes a general MOU with HPC each biennium that includes ITSS, and HPC has executed an MOU with the Texas Optometry Board regarding use of TOB staff to deliver ITSS services on behalf of HPC. Management believes this addresses the SAO's concern about non-HPC employees providing ITSS services to the Council.

The staff responsible for implementation are the Executive Director, CFO, and Systems Support Specialist.

Lastly, with regard to the concern about proper segregation between USAS and VERSA, due to the small size of the agency and the fact that there are only two staff in the accounting division, it is imperative that each accounting staff have the ability to process specific transactions into CAPPS, USAS, and VERSA in their own right. This is needed in order to meet the state Treasury three day deposit rule for monies received by the agency and process payroll and other "emergency" expenditures in the event the other accounting staff member is unable to assist or provide oversight. Thus, the agency is willing to accept the risk associated with the overlap in authority for entries into CAPPS, USAS, and VERSA.

To further illustrate this point, there are a limited number of staff that can modify payments from applicants/licensees in VERSA, through which all revenue runs, and there is a history log containing the username, date, and time that captures any changes to these payments. All online VERSA revenues are transmitted into USAS appropriations through their respective coding blocks set up in VERSA and approved by the Comptroller. VERSA payments are reconciled with USAS payments monthly by the CFO in order to prepare and submit the Texas.gov Subscription Fee Report. Any anomalies in payments would be noticed at that point and researched.

Additionally, while USAS is the agency's "system of record", all offline VERSA revenues and agency expenditures are entered into CAPPS and transmitted into USAS via file transfer. Business procedures dictate that the accountant enters revenues and expenditures into CAPPS, and releases the revenues. The CFO is the only one with security to release expenditures. While the CFO has

the security to enter and release expenditures, this only occurs in limited situations. USAS and CAPPS are reconciled monthly by the CFO.

Strengthen Controls for Regulatory Tracking System, Ch. 3: The Council should strengthen controls for its regulatory tracking system.

Management Response: The concerns identified here relate to mandating entry of city and zip codes in VERSA and failure to enter a priority level, classification, or summary for complaints in VERSA. Management agrees with the recommendations and has already taken the corrective action necessary to address these concerns. More specifically, changes have been made to the VERSA to ensure the entry of a city and zip code for applicants and licensees. Additionally, agency staff have implemented a policy whereby the priority level, classification and summary of the complaint is entered into VERSA and updated as necessary.

Management explored making the priority level, classification, and summary fields in VERSA mandatory, but such changes would have either required unanimous approval by the agencies utilizing the shared regulatory database, or a customization for the Council at an estimated cost of $24,000 to $28,000. As such, management elected to implement the aforementioned policy at zero cost.

The staff responsible for implementation are the Executive Director and CFO.

Establish Policies and Procedures for IT Functions, Ch. 3: The Council did not properly establish policies and procedures for its IT functions.

Management Response: This concern seemingly arose out of the lack of written procedures for approving and restricting access to the Council's network and regulatory system when staff are hired, change roles, or leave employment with the agency. With that understanding, management agrees with the recommendations and has already taken the corrective action necessary to address this concern.

The staff responsible for implementation is the Executive Director.

Appendix 1

Objectives, Scope, and Methodology

The following members of the State Auditor's staff performed the audit:

- Cody Bogan, CFE (Project Manager)
- Bianca F. Pineda, CFE, CGAP (Assistant Project Manager)
- Robby Webb
- Link Wilson
- Dana Musgrave, MBA, CFE (Quality Control Reviewer)
- Cesar Saldivar, CIA, CFE, CGAP (Audit Manager)

Objectives

The objectives of this audit were to determine whether the Behavioral Health Executive Council (Council) has processes and related controls to help ensure that the Council complies with applicable requirements in:

- Conducting licensing activities;
- Reviewing, investigating, and resolving complaints; and
- Making the disciplinary information of licensees available to the public.

Scope

The scope of this audit covered the Council's processes over its licensing and enforcement (complaints) activities, including the process for making licensees' disciplinary histories available to the public, from September 1, 2021, through April 30, 2023.

The scope also included a review of significant internal control components related to the Council's licensing and enforcement processes.

Methodology

We conducted this performance audit from March 2023 through August 2023 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. In addition, during the audit, matters not required to be reported in accordance with *Government Auditing Standards* were communicated to Council management for consideration.

Addressing the Audit Objectives

During the audit, we performed the following:

- Interviewed Council staff to gain an understanding of processes and controls related to licensing and enforcement activities within the audit scope.
- Identified the relevant criteria:
  - Texas Occupations Code, Chapters 501, 502, 503, 505, and 507.
  - Texas Health and Safety Code, Chapter 105.
  - Texas Administrative Code, Title 22, Parts 21, 30, 34, 35, and 41.
  - Texas Administrative Code, Title 1, Part 10, Chapter 202.
  - Department of Information Resources' *Security Control Standards Catalog,* Version 2.0.
  - Council policies, procedures, and manuals.
- Tested the Council's applications, licenses, complaints, and disciplinary actions to determine if they were accurately supported, approved, and processed in accordance with applicable requirements.
- Tested user access to the Uniform Statewide Accounting System (USAS); the Council's licensing and enforcement system, VERSA Regulation; and the Council's network.
- Tested application controls for VERSA Regulation.

- Reviewed and reconciled revenue collected for licensing and enforcement activities between the Council's financial system of record, USAS, and its regulatory system, VERSA Regulation.

Figure 1 shows the populations and samples selected for testing.

Figure 1

Populations and Samples Selected for Testing

Population	Population Size	Sample Size [a]	Sampling Methodology [h]
New Licenses (consisting of initial applications, upgrades, reinstatements, and temporary licenses)	11,872	25 random and 5 risk-based [b]	Nonstatistical Random and Risk-Based
License Renewals	48,295	25 random and 5 risk-based [c]	Nonstatistical Random and Risk-Based
Denied License Applications	80	20 random and 3 risk-based [d]	Nonstatistical Random and Risk-Based
Expired License Applications	1,482	25 random and 5 risk-based [e]	Nonstatistical Random and Risk-Based
Probable Cause Complaints	524	25 random and 5 risk-based [f]	Nonstatistical Random and Risk-Based
Non-Probable Cause Complaints	667	25 random and 5 risk-based [g]	Nonstatistical Random and Risk-Based
Disciplinary Actions	148	25 random	Nonstatistical Random

[a] A risk-based sample is not representative, and it would not be appropriate to project those test results to the population. Populations were selected to ensure review of various factors such as [b] multiple license types, [c] $0 or fee total differences, [d] different license statuses, [e] high number of days applications were open, [f] multiple dispositions or related to complaints received by SAO, and [g] high priority classifications.

[h] A nonstatistical random sample is representative. This sample design was chosen so the sample could be evaluated in the context of the population. It would be appropriate to project those test results to the population, but the accuracy of the projection cannot be measured.

Data Reliability and Completeness

To determine data reliability and completeness, auditors (1) observed the Council's extraction of requested data populations, (2) reviewed data queries and report parameters, (3) analyzed the populations for reasonableness and completeness, and (4) tested VERSA Regulation user access and application

controls. Auditors determined that the following data sets were sufficiently reliable for the purposes of the audit:

- Population of the Council's license applications that were processed between September 1, 2021, and April 30, 2023.
- Population of the Council's complaints that were closed between September 1, 2021, and April 30, 2023.

Report Ratings

In determining the ratings of audit findings, auditors considered factors such as financial impact; potential failure to meet program/function objectives; noncompliance with state statute(s), rules, regulations, and other requirements or criteria; and the inadequacy of the design and/or operating effectiveness of internal controls. In addition, evidence of potential fraud, waste, or abuse; significant control environment issues; and little to no corrective action for issues previously identified could increase the ratings for audit findings. Auditors also identified and considered other factors when appropriate.

Copies of this report have been distributed to the following:

Legislative Audit Committee

The Honorable Dan Patrick, Lieutenant Governor, Joint Chair

The Honorable Dade Phelan, Speaker of the House, Joint Chair

The Honorable Joan Huffman, Senate Finance Committee

The Honorable Robert Nichols, Member, Texas Senate

The Honorable Greg Bonnen, House Appropriations Committee

The Honorable Morgan Meyer, House Ways and Means Committee

Office of the Governor

The Honorable Greg Abbott, Governor

Behavioral Health Executive Council

Members of the Behavioral Health Executive Council

Mr. Darrel D. Spinks, Executive Director