An Audit Report on

Cybersecurity at the Texas Medical Board

May 2020

Report No. 20-031

State Auditor's Office reports are available on the Internet at http://www.sao.texas.gov/.

An Audit Report on

Cybersecurity at the Texas Medical Board

SAO Report No. 20-031
May 2020

Overall Conclusion

The Texas Medical Board (Board) should strengthen its information security program to meet statutory requirements and the Department of Information Resources' (DIR) information security standards (see text box). Specifically:

- The Board did not define and classify the types of data it manages, prioritize its information technology (IT) assets based on their importance, perform a risk assessment, or identify a risk management strategy. That data includes confidential information on licenses for physicians, physicians' assistants, and other medical practitioners.
- Although the Board completed its 2018 Security Plan as required, it should strengthen its documentation of management oversight, staff training, and policies and procedures.
- While the Board had controls in place to protect its network from logical, environmental, and physical threats, it did not always appropriately restrict user access to key information resources. Auditors also identified areas for improvement related to the Board's controls over its change management.

Information Security Criteria

Texas Government Code provides requirements for information security, and the Department of Information Resources (DIR) has established the minimum baseline for information security standards for state agencies. Specifically:

- Texas Government Code, Chapter 2054, contains requirements relating to information security plans, breach notifications, information technology infrastructure reporting, and vulnerability reporting.
- Title 1, Texas Administrative Code, Chapter 202, establishes DIR's baseline information security standards for state agencies. Those standards outline the requirements regarding the responsibilities of the agency head, the information security officer, and staff, as well as requirements for information security programs and risk management.
- DIR's *Security Controls Standards Catalog* (Catalog) specifies the minimum requirements for specific information security controls that state agencies must implement. That Catalog aligns with the National Institute of Standards and Technology's (NIST) security and privacy standards.
- DIR's *Texas Cybersecurity Framework Control Objectives and Definitions* contains 46 cybersecurity control objectives for state agencies. That framework, which is based on NIST's *Framework for Improving Critical Infrastructure Cybersecurity*, is divided into five core functions (identify, protect, detect, respond, and recover). State agencies report to DIR on those security objectives biennially through their information security plans.

Sources: The Texas Government Code, the Texas Administrative Code, and DIR.

The Board also had significant weaknesses in its controls that weaken its ability to address cybersecurity incidents. Auditors communicated details about the identified weaknesses related to sensitive information technology issues separately to the Board in writing.

Pursuant to Standard 9.61 of the U.S. Government Accountability Office's *Government Auditing Standards*, certain information was omitted from this report because that information was deemed to present potential risks related to public safety, security, or the disclosure of private or confidential data. Under the

This audit was conducted in accordance with Texas Government Code, Section 321.0134.

For more information regarding this report, please contact Michael Simon, Audit Manager, or Lisa Collier, First Assistant State Auditor, at (512) 936-9500.

provisions of Texas Government Code, Section 552.139, the omitted information is also exempt from the requirements of the Texas Public Information Act.

Table 1 presents a summary of the findings in this report and the related issue rating. (See Appendix 2 for more information about the issue rating classifications and descriptions.)

Table 1

Summary of Chapters/Subchapters and Related Issue Ratings		
Chapter/ Subchapter	**Title**	**Issue Rating [a]**
1	Background on State of Texas Information Security Standards	Not Rated
2	The Board Should Strengthen Its Information Technology Governance by Implementing a Process to Identify and Manage Information Security Risks and Updating Policies and Procedures to Reflect Requirements and Practices	High
3-A	The Board Had Controls in Place to Ensure Network Security and IT Asset Physical Security; However It Should Improve Its Policies for the Encryption of Data	Medium
3-B	The Board Did Not Always Ensure That User Access to Critical Information Systems Was Appropriate and Based on Job Duties	High
3-C	The Board Had Processes in Place to Ensure That Information Security Was Incorporated in the Development of Its Information Systems; However, It Should Establish Change Management Processes	Medium
4	The Board Had Significant Weaknesses in Its Controls to Address Cybersecurity Incidents	**Priority**

[a] A chapter/subchapter is rated **Priority** if the 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 and reduce risks to the audited entity.

A chapter/subchapter is rated **High** if the 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 and reduce risks to the audited entity.

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

A chapter/subchapter is rated **Low** if 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.

Auditors communicated other, less significant issues separately in writing to Board management.

Summary of Management's Response

At the end of each chapter in this report, auditors made recommendations to address the issues identified during this audit. The Board agreed with the recommendations in this report; however, it identified some limitations in its ability to implement some recommendations.

Audit Objective and Scope

The objective of this audit was to determine whether the Board has implemented information system security standards and related controls in compliance with the requirements of DIR's information security standards.

The scope of this audit covered selected information security standards and controls over the Board's significant information technology systems and assets from September 1, 2018, through December 31, 2019. The audit methodology was structured to align with the five cybersecurity functional areas (identify, protect, detect, respond, and recover) identified in DIR's *Texas Cybersecurity Framework Control Objectives and Definitions*, which is based on the National Institute of Standards and Technology's (NIST) *Framework for Improving Critical Infrastructure Cybersecurity*.

Contents

Detailed Results

Appendices

Detailed Results

Chapter 1

Background on State of Texas Information Security Standards

Auditors reviewed the Texas Medical Board's (Board) compliance with standard requirements and guidance that all state entities must follow to protect their critical information resources from cybersecurity threats. Those requirements and guidance are included in Title 1, Texas Administrative Code, Chapter 202, the *Texas Cybersecurity Framework Control Objectives and Definitions* (*Framework*), and *Security Control Standards Catalog* (*Catalog*). The requirements were developed by the Department of Information Resources (DIR).

Title 1, Texas Administrative Code, Chapter 202

Title 1, Texas Administrative Code, Chapter 202, outlines specific requirements for key personnel at state agencies and higher education institutions, as well as overall requirements for those entities to develop an information security program.

Specifically, it includes requirements related to (1) the responsibilities of an agency's head, information security officer, and staff, (2) security reporting, (3) implementing an information security program, and (4) managing security risks.

Texas Cybersecurity Framework Control Objectives and Definitions

The *Framework* was developed in response to Texas Government Code, Section 2054.059, to provide an overall framework to be used by state agencies to secure their information resources from cybersecurity threats.

The *Framework* was based on the National Institute of Standards and Technology's *Framework for Improving Critical Infrastructure Cybersecurity* and is divided into five concurrent and continuous functions: Identify, Protect, Detect, Respond, and Recover. Within these five areas, DIR defined 46 security objectives, as of 2020.

Table 2 on the next page provides descriptions of the five functional areas.

Table 2

Texas Cybersecurity Framework Control Objectives and Definitions		
Functional Area	**Description of Functional Area**	**Report Chapter Discussing Functional Area**
Identify	What processes and assets need protection? The Identify functional area assists in developing an organizational understanding of managing cybersecurity risk to systems, people, assets, data, and capabilities.	Chapter 2
Protect	What safeguards are available? The Protect functional area supports the ability to limit or contain the impact of potential cybersecurity events and develop and implement appropriate safeguards to ensure delivery of critical services.	Chapter 3
Detect	What techniques can identify incidents? The Detect functional area defines the appropriate activities to identify the occurrence of a cybersecurity event in a timely manner.	Chapter 4
Respond	What techniques can contain impacts of incidents? The Respond functional area defines appropriate activities to take action regarding a detected cybersecurity incident to minimize impact.	Chapter 4
Recover	What techniques can restore capabilities? The Recover functional area identifies appropriate activities to maintain plans for resilience and to restore services impaired during cybersecurity incidents.	Chapter 4

Sources: *Texas Cybersecurity Framework Control Objectives and Definitions* and National Institute of Standards and Technology's *Framework for Improving Critical Infrastructure Cybersecurity*.

Security Control Standards Catalog

The *Catalog* specifies the minimum information security requirements that state agencies and higher education institutions must comply with to provide the appropriate levels of information security according to risk levels. The *Catalog* specifies the purpose, levels of risk, implementation overview, and implementation examples for each control activity.

The *Catalog* defines a total of 282 controls. They include controls related to account management; separation of duties; the principle of least privilege; security awareness training; audit events; contingency planning; identification and authentication; incident handling; risk assessment; and malicious code protection.

Chapter 2

The Board Should Strengthen Its Information Technology Governance by Implementing a Process to Identify and Manage Information Security Risks and Updating Policies and Procedures to Reflect Requirements and Practices

Chapter 2 Rating:

High [1]

The Texas Medical Board (Board) should strengthen its information security governance to perform steps that will assist the Board in identifying significant cybersecurity risks to its systems, people, assets, data, and capabilities (see text box for more information about the *Framework*'s Identify functional area).

Identify Functional Area

This functional area contains requirements to help agencies develop an understanding of managing cybersecurity risks to their systems, people, assets, data, and capabilities.

The security objectives for the Identify function include data classification; critical information asset inventory; enterprise security policy, standards and guidelines; information security risk management; and security oversight and governance.

Sources: DIR's *Texas Cybersecurity Framework Control Objectives and Definitions*.

Specifically, the Board should:

- Define and classify the types of data it manages;
- Prioritize which information technology (IT) assets are most critical to its operations; and
- Perform a risk assessment of its information and information systems.

In addition, while the Board performed other key activities such as establishing information security policies and procedures, it should improve its documentation of those activities to further strengthen its ability to identify and manage cybersecurity risks. For example, the Board should regularly review its policies and procedures for needed updates and document whether services provided by a third-party vendor meet security needs.

Data Classification Requirements

The Texas Administrative Code requires state agencies to define all information classification categories, except for the Confidential Information category, and establish controls for each.

According to DIR, classifying data allows agencies to make more efficient security decisions because it identifies and communicates the minimum level of protection required for any piece of data, as well as the individuals who may view that data.

Sources: Title 1, Texas Administrative Code, Section 202.24, and DIR.

The Board did not classify its data or identify and assess risks to its IT assets to appropriately develop and implement a risk management strategy.

Data Classification and IT Asset Prioritization. The Board did not define and document its information classification categories or classify its data to identify the most critical and sensitive data, as required by Title 1, Texas Administrative Code, Section 202.24 (see text box for more information

[1] The risk related to the issues discussed in Chapter 2 is rated as High because they 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 and reduce risks to the audited entity.

about data classification requirements). In addition, the Board did not document its prioritization of IT assets as required by DIR's *Framework*. All IT assets should be prioritized based on their relative criticality to the Board's operations. For example, networking equipment may be a critical IT asset. Data classification and IT asset prioritization are necessary for the Board to (1) identify its security needs based on statutory and regulatory requirements and business needs and (2) define its information security standards and policies accordingly.

Risk Assessment Requirements

An agency's IT risk assessment should document the ranking of inherent risks and the frequency of future risk assessments.

DIR defines risks as the measure of the extent to which an entity is threatened by a potential circumstance or event. Specifically, risks are typically a measure of (1) the adverse impacts that would arise if the circumstance or event occurs; and (2) the likelihood of occurrence.

Sources: Title 1, Texas Administrative Code, Section 202.25, and DIR.

Risk Assessment. The Board did not perform and document its identification and assessment of risks to its information and information systems as required by Title 1, Texas Administrative Code, Section 202.25 (see text box for information about risk assessment requirements). A risk assessment would help the agency determine the most serious risks to its information resources, including critical data and IT assets, and establish controls to mitigate those risks. However, as discussed above, the Board's lack of data classification and IT asset prioritization could hinder its ability to perform a risk assessment and establish a risk management strategy.

Not classifying its data, prioritizing its IT assets, or assessing its IT security risks as required decreases the Board's ability to design and establish an effective information security program.

The Board did not develop a data use agreement for staff as required by the Texas Government Code.

The Board did not have a data use agreement in place to be reviewed and signed by Board staff as required by Texas Government Code, Section 2054.135 (see text box for more information on data use requirements). That agreement should be distributed to and signed by employees who handle sensitive information, such as financial, medical, or personnel data.

Not having an appropriate data use agreement in place increases the risk that staff will not be aware of the types of data available to them through the Board's information systems and the authorized uses and purposes of that data.

Data Use Agreement Requirements

Texas Government Code, Section 2054.135, requires state agencies to (a) develop a data use agreement that meets their particular needs and is consistent with DIR's standards; (b) update the agreement at least biennially; (c) distribute the agreement and any updates to employees who handle sensitive information, including financial, medical, personnel, or student data and require those employees to sign the agreement; and (d) to the extent possible, provide those employees with cybersecurity awareness training to coincide with the distribution of the agreement.

DIR has provided a sample data use agreement for state agencies to use on its website.

Sources: Texas Government Code, Section 2054.135, and DIR.

The Board did not document an assessment of whether services provided by a third-party vendor met security needs.

The Board asserted that it obtained a third-party cloud[2] services vendor to host some of its information resources using a contract offered through DIR for IT services. However, the Board could not provide documentation showing any analyses it performed assessing whether the vendor could provide contracted services efficiently and effectively to meet the Board's security needs as required by DIR's *Framework* and the *Catalog*. As a result, auditors were unable to determine whether the Board performed these analyses. Not determining and documenting whether vendors will meet specific needs increases the risk that the services provided will be insufficient.

While the Board's governance structure was appropriate, documentation supporting required management oversight and staff training was lacking.

Oversight and Governance. The Board asserted that its governance structure ensured that its executive director was the immediate supervisor of its IT manager, who also served as its information security officer. This structure increases executive management's ability to oversee the information security program (see text box for more information on security oversight and governance).

Security Oversight and Governance

DIR's *Framework* defines security oversight and governance as the set of responsibilities and practices exercised by an entity's board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise's resources are used responsibly.

Source: DIR's *Texas Cybersecurity Framework Control Objectives and Definitions*.

Cybersecurity Training. While the Board provided some security awareness materials to staff during the scope of this audit, it did not have a documented security training program to ensure that staff and executive management received adequate training based on their roles, as required by the *Catalog*.

A documented training program for Board staff and executive management would help ensure that (1) all employees with access to sensitive information are aware of cybersecurity threats and privacy risks and (2) executive management has the tools necessary to provide sufficient prioritization, oversight, and monitoring of the Board's information security program.

While the Board had policies and procedures for most required security controls, it did not review them regularly for any necessary updates.

While the Board had policies and procedures addressing 11 (73.3 percent) of the 15 control activities required by DIR's *Catalog*, it did not periodically review and revise them. Specifically, 19 (90.5 percent) of 21 policies

[2] Cloud services refers to the delivery of computing services, including for servers, storage, databases, networking, and software, over the Internet.

addressing the 11 control activities audited had not been reviewed or updated since 2014. The Board approved and executed the remaining two in 2017. As a result of the lack of review and revision, some of those policies and procedures no longer aligned with the Board's processes. For example, its documented system development policy did not correspond to its current system development practices.

Not having a process to regularly review and update policies and procedures increases the risk that the Board's controls will not remain sufficient to mitigate changing information security risks.

The Board completed its biennial security plan in 2018, as required.

The Board completed its biennial security plan in 2018 and submitted it to DIR, as required. The plan requires the Board to assess its information security program against the objectives from DIR's *Framework* using a template provided by DIR.

Recommendations

The Board should strengthen its information security program to ensure compliance with statute and DIR's minimum standards, including:

- Defining and documenting its information classification categories and performing and documenting its data classification.
- Performing and documenting its IT asset prioritization.
- Performing and documenting a risk assessment and establishing and documenting a risk management strategy.
- Developing and implementing a data use agreement as required by Texas Government Code, Section 2054.135.
- Performing and documenting an analysis to determine whether third-party vendors are capable of meeting its needs.
- Implementing a documented security training program for all personnel, including role-based security training and security awareness and privacy training.
- Establishing a process to regularly review, approve, and update its information security policies, standards, and procedures.

Management's Response

Recommendations

The Board should strengthen its information security program to ensure compliance with statute and DIR's minimum standards, including:

1. *Defining and documenting its information classification categories and performing and documenting its data classification.*

2. *Performing and documenting its IT asset prioritization.*

3. *Performing and documenting a risk assessment and establishing and documenting a risk management strategy.*

4. *Developing and implementing a data use agreement as required by Texas Government Code, Section 2054.135.*

5. *Performing and documenting an analysis to determine whether third-party vendors are capable of meeting its needs.*

6. *Implementing a documented security training program for all personnel, including role-based security training and security awareness and privacy training.*

7. *Establishing a process to regularly review, approve, and update its information security policies, standards, and procedures.*

Management Response

Management agrees with the facts used by SAO to produce the recommendations in Chapter 2.

Management will implement recommendation 4 and will be completed by the end of 12/31/20. The responsible party is the IT Manager.

Management will develop the process from recommendation 7 by 8/31/21. The responsible party is the IT Manager.

Management believes TMB needs more resources before it can consider implementing recommendations 1-3, 5-6 without impacting the agency's mission and service delivery. The work of reviewing and updating policies and procedures in recommendation 7 requires additional resources. The agency will submit a LAR request for the additional resources.

Chapter 3

The Board Should Strengthen Its Controls Designed to Prevent Cybersecurity Threats to Its Information Systems

While the Board developed some controls to limit the impact of cybersecurity threats to its information systems, improvements and enhancements are needed to that control structure to ensure that the Board's information systems are adequately protected (see text box for more information on the Protect area requirements).

Protect Functional Area

The Protect functional area contains requirements to help agencies limit or contain the impact of potential cybersecurity events and develop and implement appropriate safeguards to ensure delivery of critical services.

The security objectives for the Protect function include secure configuration management; change management; physical environmental protection; access control; account management; and network access and perimeter controls.

Sources: DIR's *Texas Cybersecurity Framework Control Objectives and Definitions*.

The Board had controls and processes in place to ensure network security and the physical security of IT assets. However, it did not (1) have a documented process to consistently manage the encryption of critical data and assets or (2) consistently restrict employees' user access appropriately.

In addition, while the Board ensured that it included appropriate personnel in information system development, it should ensure that changes to its information systems are consistently tracked, documented, approved, and tested.

Improving its controls in the above areas would help to reduce the risk of (1) unauthorized or unintentional modifications to the Board's information systems and data and (2) data exposure in the event of a breach.

Chapter 3-A

The Board Had Controls in Place to Ensure Network Security and IT Asset Physical Security; However, It Should Improve Its Policies for the Encryption of Data

Chapter 3-A Rating:

Medium [3]

The Board had controls in place to secure its network and IT assets from logical, environmental, and physical security threats. It also ensured that users accessed information resources with unique user accounts and had adequate authentication settings. However, it should establish a documented process to manage the encryption of critical data and IT assets.

Network Security. The Board had controls in place to mitigate the risk of unauthorized external access to its network and to IT assets. Network access controls included a firewall, an intrusion-prevention system designed to detect and prevent unauthorized external access, and encryption to protect authorized remote access to its network from security threats.

The Board also had controls to mitigate environmental threats and restrict physical access to network hardware and other critical IT assets. Those controls included restricting access to Board servers and other network hardware, which are located in a secured room with regulated temperature and fire-suppression equipment.

User Authentication. Users accessed key applications and systems using unique user accounts that are authenticated through the Board's network. The Board also had controls in place to enforce user authentication settings, including enforcing password settings, for those user accounts.

Data Encryption. The Board had controls in place to encrypt data being transmitted through remote connections and its policies required portable devices containing sensitive data to be encrypted. However, the Board did not have processes in place to ensure that all data and devices are encrypted and should improve its policies and procedures to help manage the encryption of data in a consistent manner. Specifically, the Board's policies did not require that all portable devices or data stored in its databases or other devices be encrypted. Having policies and procedures that requires consistent encryption of its data and IT assets would help the Board reduce the risk of data exposure in the event of a breach.

[3] The risk related to the issues discussed in Chapter 3-A is rated as Medium because they present risks or effects that if not addressed could moderately affect the audited entity's ability to effectively administer program(s)/function(s) audited. Action is needed to address the noted concern and reduce risks to a more desirable level.

Recommendation

The Board should update its processes, policies, and procedures to establish a consistent process to manage the encryption of its data and IT assets.

Management's Response

Management agrees with the facts used by SAO to produce recommendation 3-A.

Implementing recommendation 3-A will be completed the by 12/31/21. The responsible party is the IT Manager. If the agency determines that encryption management tools are necessary, implementation will be partially dependent on funding.

Chapter 3-B

The Board Did Not Always Ensure That User Access to Critical Information Systems Was Appropriate Based on Job Duties

Chapter 3-B Rating:

High [4]

The Board did not always appropriately restrict user access to key information resources. The *Catalog* requires state entities to restrict access to only the level necessary to accomplish the users' job duties, known as the "principle of least privilege." User access must also ensure adequate separation of duties (see text box for more information).

Principle of Least Privilege and Separation of Duties

According to the *Catalog*, state entities should employ controls in accordance with the principle of least privilege and to ensure separation of duties by:

- Allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.
- Ensuring adequate controls and separation of duties for tasks that are susceptible to fraudulent or other unauthorized activity.

Source: The *Catalog*.

However, several of the Board's information technology employees had administrative access to all of the Board's servers, which did not align with the principle of least privilege. Other employees had access that increased the risk of unauthorized activities. Because the Board handles sensitive and confidential information and processes financial transactions, it is important that system access is appropriate.

The Board did ensure that user access to agency databases was appropriate based on the users' job duties.

[4] The risk related to the issues discussed in Chapter 3-B is rated as High because the 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 and reduce risks to the audited entity.

The Board did not always ensure that information resource users had access to its network and financial systems that was appropriate to their job duties and provided adequate separation of duties.

Network Access. Of the 11 users with network domain administrative access, 5 (45 percent) did not require that access level. While the Board asserted that those five employees required administrative access to certain servers to perform their job duties, domain administrative rights provide significant read/write access to all servers within the Board's network. As a result, that level of access would not be appropriate based on their job duties. For example, administrative access to the server hosting the Board's email services would not be necessary for a programmer's assigned duties. That level of access also enables the user to make edits to the Board's servers, including editing logs and creating/deleting user accounts.

Not appropriately restricting access for users increases the risk of unintentional or unauthorized modification or misuse of the Board's information resources.

Financial Systems. Two users had access in both the Centralized Accounting and Payroll/Personnel System and the Uniform Statewide Accounting System (USAS) that allowed those users to both create and approve transactions. As a result, they could bypass separation of duties controls, which increases the risk of erroneous or unauthorized transactions. Auditors did not identify any fiscal year 2019 transactions that were both created and approved by a single user.

The Board had controls to ensure that access to its databases was appropriate to users' job duties.

The Board ensured that user access to databases for key systems was appropriate to the users' job duties. Specifically, the Board ensured that administrative access to those databases was restricted to an account that the Board asserted was assigned to its database administrator based on the job duties of that position.

Recommendation

The Board should strengthen its access controls to ensure that user access is assigned based on the principle of least privilege and provides adequate separation of duties.

Management's Response

Management agrees with the facts used by the SAO to produce recommendation 3-B.

Management believes the agency cannot implement recommendation 3-B without impacting the agency's mission, service delivery or Continuity of Operations. The agency needs additional resources to ensure adequate segregation of duties. The agency will submit a LAR request for additional resources. As opportunities arise, the agency will strengthen user access controls without impacting ongoing agency operations or Continuity of Operations.

Chapter 3-C

The Board Had Processes in Place to Ensure That Information Security Was Incorporated in the Development of Its Information Systems; However, It Should Establish Change Management Processes

Chapter 3-C Rating:
Medium [5]

The Board had processes to ensure that information security considerations were included in its development of information systems. However, it should establish consistent change management processes for its information systems.

System Development

The Board's information system development processes incorporate Agile Development principles (see text box for more information about Agile Development). The Board's policies governing system development also require it to follow DIR's *Texas Project Delivery Framework* [6] to adequately document system development. In addition, for the system development project that auditors reviewed, the Board asserted that developers obtained input from key stakeholders.

Agile Development

Agile Development is a methodology for managing software development projects.

The Agile Alliance, a nonprofit organization, describes 12 principles underlying its *Agile Manifesto*. That manifesto rolls those 12 principles into four overarching ideals: (1) individuals and interactions over processes and tools, (2) working software over comprehensive documentation, (3) customer collaboration over contract negotiation, and (4) responding to change over following a plan.

Source: The Agile Alliance's *Agile Manifesto*.

[5] The risk related to the issues discussed in Chapter 3-C is rated as Medium because they present risks or effects that if not addressed could moderately affect the audited entity's ability to effectively administer program(s)/function(s) audited. Action is needed to address the noted concern and reduce risks to a more desirable level.

[6] The *Texas Project Delivery Framework* is designed for major, large-scale information technology projects. DIR has developed several templates that it intends for state entities following the *Texas Project Delivery Framework* to use to help ensure that their projects stay on track and outcomes are measurable.

Development of Licensing and Enforcement System. As of December 2019, the Board asserted that it was developing a new licensing and enforcement system with associated online components to be made available to licensees and members of the public.[7] The Board maintained email communications for that development project demonstrating that it ensured that key personnel were involved, including personnel responsible for ensuring that information security considerations and agency needs were assessed and incorporated into the planning and design. Specifically, the information security officer, executive director, and managers representing end users of the system were included in those communications discussing specific aspects of the project.

Change Management

The Board did not have a consistent process to track and document changes made to its information resources. As a result, the Board cannot verify that all changes made to information systems were adequately tested and approved as required by the *Catalog*. In addition, programmers responsible for developing changes had the ability to implement those changes (see Chapter 3-B for more details). Not maintaining consistent documentation and adequate separation of duties increases the risk that (1) the Board will not be aware of all changes being made and (2) changes that compromise system data and security are implemented.

Recommendations

The Board should develop and implement a process to track and document changes made to information systems, including testing and approvals, and ensure adequate separation of duties.

Management's Response

Management agrees with the facts used by SAO to produce recommendation 3-C.

Management believes that implementing recommendation 3-C will negatively impact the Agency's mission and operations. Additional resources are required to offset the time spent on the recommended documentation activities. Additional resources are required to ensure adequate segregation of duties. The agency will submit a LAR request for additional resources.

[7] The Board did not report to the Legislative Budget Board that the total estimated costs of the Board's licensing and enforcement system exceeded $5 million. As a result, it was not classified as a major project as defined by Texas Government Code, Section 2054.003, and the Board was not required to complete and submit *Texas Project Delivery Framework* documentation to the Quality Assurance Team.

Chapter 4

The Board Had Significant Weaknesses in Its Controls to Address Cybersecurity Incidents

Chapter 4 Rating:

Priority [8]

Auditors identified significant weaknesses in the Board's ability to address cybersecurity incidents. To minimize security risks, auditors communicated details about the identified weaknesses separately to the Board's management, in writing.

Pursuant to Standard 9.61 of the U.S. Government Accountability Office's *Generally Accepted Government Auditing Standards*, certain information was omitted from this report because that information was deemed to present potential risks related to public safety, security, or the disclosure of private or confidential data. Under the provisions of Texas Government Code, Section 552.139, the omitted information is also exempt from the requirements of the Texas Public Information Act.

[8] The risk related to the issues discussed in Chapter 4 is rated as Priority because the 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 and reduce risks to the audited entity.

Appendices

Appendix 1

Objective, Scope, and Methodology

Objective

The objective of this audit was to determine whether the Texas Medical Board has implemented information security standards and related controls in compliance with the requirements of the Department of Information Resources' (DIR) information security standards.

Scope

The scope of this audit covered selected information security standards and controls over the Board's significant information technology systems and assets from September 1, 2018, through December 31, 2019.

Methodology

The audit methodology included gaining an understanding of the Board's information security standards and related controls, collecting and reviewing policies and procedures, collecting documentation related to information security controls, performing tests and other procedures, and analyzing and evaluating the results of those tests.

The audit methodology was structured to align with the five cybersecurity functional areas (identify, protect, detect, respond, and recover) identified in DIR's *Texas Cybersecurity Framework Control Objectives and Definitions*, which is based on the National Institute of Standards and Technology's (NIST) *Framework for Improving Critical Infrastructure Cybersecurity*.

Data Reliability and Completeness

- Auditors obtained data sets from the Board to review user access for significant information technology systems. To determine whether that data was valid and complete, auditors (1) observed the Board's extraction of user access data sets and (2) reviewed user access.
- Auditors determined that the data was sufficiently reliable for the purpose of this audit.

Information collected and reviewed included the following:

- The Board's policies and procedures.
- Supporting documentation related to the Board's information security plan and standards.
- Supporting documentation related to controls over the Board's significant information technology systems.
- User access data for significant information technology systems.
- Password parameters for significant information technology systems.
- The Board's Agency Strategic Plan 2019–2023.
- Board meeting minutes.

Procedures and tests conducted included the following:

- Interviewing the Board's management and staff.
- Reviewing policies, procedures, and supporting documentation and observing controls over the Board's significant information technology systems and assets for compliance with statute and DIR's information security standards.
- Reviewing Board meeting minutes and training requirements to determine the key responsibilities and levels of oversight in managing information security risks for the information technology staff, executive management, and the governing board at the Board.
- Performing a walkthrough of the Board's server room to determine whether physical security controls were in place.
- Testing logical access to the Board's significant information technology systems to determine whether system access permissions for users were appropriate.
- Testing password settings for significant information technology systems to determine compliance with DIR's minimum standards.

Criteria used included the following:

- Texas Government Code, Chapter 2054.
- Title 1, Texas Administrative Code, Chapter 202.
- DIR's *Security Control Standards Catalog*, Version 1.3.
- DIR's *Texas Cybersecurity Framework Control Objectives and Definitions*.
- The Board's policies and procedures.

Project Information

Audit fieldwork was conducted from September 2019 through January 2020. We conducted this performance audit 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.

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

- Scott Armstrong, CGAP (Project Manager)
- Michael Bennett (Assistant Project Manager)
- Jennifer Fries, MS
- Joseph A. Kozak, CPA, CISA
- Derek Lopez, MBA
- Mary Ann Wise, CPA, CFE (Quality Control Reviewer)
- Michael A. Simon, MBA, CGAP (Audit Manager)

Appendix 2

Issue Rating Classifications and Descriptions

Auditors used professional judgment and rated the audit findings identified in this report. Those issue ratings are summarized in the report chapters/sub-chapters. The issue ratings were determined based on the degree of risk or effect of the findings in relation to the audit objective(s).

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.

Table 3 provides a description of the issue ratings presented in this report.

Table 3

Summary of Issue Ratings	
Issue Rating	**Description of Rating**
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.
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.
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.
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.

Appendix 3

Internal Control Components

Internal control is a process used by management to help an entity achieve its objectives. Government Auditing Standards require auditors to assess internal control when internal control is significant to the audit objectives. The Committee of Sponsoring Organizations of the Treadway Commission (COSO) established a framework for 5 integrated components and 17 principles of internal control, which are listed in Table 4.

Table 4

Internal Control Components and Principles		
Component	**Component Description**	**Principles**
Control Environment	The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure.	▪ The organization demonstrates a commitment to integrity and ethical values. ▪ The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control. ▪ Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives. ▪ The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives. ▪ The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.
Risk Assessment	Risk assessment is the entity's identification and analysis of risks relevant to achievement of its objectives, forming a basis for determining how the risks should be managed.	▪ The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives. ▪ The organization identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed. ▪ The organization considers the potential for fraud in assessing risks to the achievement of objectives. ▪ The organization identifies and assesses changes that could significantly impact the system of internal control.
Control Activities	Control activities are the policies and procedures that help ensure that management's directives are carried out.	▪ The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels. ▪ The organization selects and develops general control activities over technology to support the achievement of objectives. ▪ The organization deploys control activities through policies that establish what is expected and procedures that put policies into action.
Information and Communication	Information and communication are the identification, capture, and exchange of information in a form and time frame that enable people to carry out their responsibilities.	▪ The organization obtains or generates and uses relevant, quality information to support the functioning of internal control. ▪ The organization internally communicates information, including objectives and responsibilities

Internal Control Components and Principles		
Component	**Component Description**	**Principles**
		for internal control, necessary to support the functioning of internal control. ▪ The organization communicates with external parties regarding matters affecting the functioning of internal control.
Monitoring Activities	Monitoring is a process that assesses the quality of internal control performance over time.	▪ The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning. ▪ The organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.

Source: Internal Control – Integrated Framework, Committee of Sponsoring Organizations of the Treadway Commission, May 2013.

Copies of this report have been distributed to the following:

Legislative Audit Committee

The Honorable Dan Patrick, Lieutenant Governor, Joint Chair
The Honorable Dennis Bonnen, Speaker of the House, Joint Chair
The Honorable Jane Nelson, Senate Finance Committee
The Honorable Robert Nichols, Member, Texas Senate
The Honorable Giovanni Capriglione, House Appropriations Committee
The Honorable Dustin Burrows, House Ways and Means Committee

Office of the Governor

The Honorable Greg Abbott, Governor

Texas Medical Board

Members of the Texas Medical Board
- Dr. Sherif Z. Zaafran, President
- Mr. Arun Agarwal
- Ms. Sharon J. Barnes
- Dr. Devinder S. Bhatia
- Mr. Michael E. Cokinos
- Dr. George L. De Loach, D.O.
- Dr. Kandace B. Farmer, D.O.
- Mr. Robert Gracia
- Ms. Tomeka M. Herod
- Dr. J. Scott Holliday, MBA
- Dr. Jeffrey L. Luna
- Dr. Robert D. Martinez
- Ms. Linda Molina, J.D.
- Ms. LuAnn R. Morgan
- Dr. Jayaram B. Naidu
- Dr. Satish Nayak
- Dr. Manuel M. Quinones, Jr.
- Dr. Jason K. Tibbels
- Dr. David G. Vanderweide

Mr. Stephen Brint Carlton, Executive Director