An Audit Report on

Cybersecurity at the School for the Deaf

February 2019

Report No. 19-031

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

An Audit Report on

Cybersecurity at the School for the Deaf

SAO Report No. 19-031
February 2019

Overall Conclusion

The School for the Deaf (School) should strengthen its information security program to meet statutory requirements and the Department of Information Resources' (DIR) information security standards. The School did not adequately establish and document its information security policies, standards, and procedures, and it did not perform the required risk assessment of its information systems.

As a result, the School did not implement certain information security controls in accordance with statute and DIR's minimum standards (see text box). Specifically, the School did not implement controls to ensure that external service providers meet its information security requirements. Auditors also identified significant weaknesses in the School's controls over access to its information systems. The identified weaknesses place the School's data at risk of unauthorized or inappropriate access, use, and modification.

In addition, auditors identified areas for improvement related to the School's controls over its system configurations; system development and change management; and incident detection, response, and recovery planning.

Auditors communicated details about the identified weaknesses related to access and other sensitive information technology issues separately to the School in writing.

Pursuant to Standard 7.41 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 provisions of Texas Government Code, Section 552.139, the omitted information is also exempt from the requirements of the Texas Public Information Act.

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 40 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.

This audit was conducted in accordance with Texas Government Code, Section 321.0132.

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

Table 1 presents a summary of the findings in this report and the related issue ratings. (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-A	The School Should Establish and Document Its Information Security Policies, Standards, and Procedures, and It Should Implement a Process to Identify and Manage Its Information Security Risks	Priority
1-B	The School Should Strengthen Its Processes and Controls to Ensure That External Service Providers Meet Its Information Security Requirements	High
2-A	The School Should Establish and Document Its System Configurations and Its Processes for System Development and Change Management	Medium
2-B	The School Should Strengthen Access Controls Over Its Information Systems	High
3	Although the School Implemented Network and Physical Security Controls, It Should Strengthen Certain Controls Over Its Incident Detection, Response, and Recovery Planning	Medium

[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 the 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 School management.

Summary of Management's Response

At the end of certain chapters in this report, auditors made recommendations to address the issues identified during this audit. The School agreed with the recommendations in this report. The School's detailed management responses are presented at the end of each chapter in this report. The School's management response to the Overall Conclusion section above is presented in Appendix 3.

Audit Objective and Scope

The objective of this audit was to determine whether the School 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 system security standards and controls over the School's significant information technology systems and assets from September 1, 2017, through December 31, 2018.

Contents

Detailed Results

Appendices

Detailed Results

Chapter 1

The School Should Strengthen Its Information Technology Governance and External Service Provider Management

The School for the Deaf (School) should strengthen its information security program to ensure that it complies with statutory requirements and the Department of Information Resources' (DIR) minimum information security standards. The School did not define and classify the types of data it managed, perform a risk assessment, or identify its risk management strategy. As a result, the School did not adequately establish and document its information security policies, standards, and procedures, including those related to its management of external service providers.

In addition, the School's governance structure should increase its oversight of information security risks and implement a training program to ensure that the School's information security program complies with statute and DIR's requirements.

Chapter 1-A

The School Should Establish and Document Its Information Security Policies, Standards, and Procedures, and It Should Implement a Process to Identify and Manage Its Information Security Risks

Chapter 1-A Rating:

Priority[1]

The School should develop appropriate information security policies, standards, and procedures as required by DIR's minimum standards. To facilitate the development of those policies, standards, and procedures, the School should implement certain information security processes, including classifying its data, performing a risk assessment, and establishing a training program to increase the School's understanding of information security risks and DIR's requirements.

Establishment of Security Policies, Standards, and Procedures. The School did not develop and document its information security policies, standards, and procedures for several key information security areas, such as risk assessment, security awareness and training, system and services acquisition, and configuration management.

[1] The risk related to the issues discussed in Chapter 1-A 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.

Although the School had an acceptable use policy and procedures related to account management, those documents did not meet DIR's minimum standards for information security policies and procedures. In addition, those documents did not incorporate federal and state statutory requirements related to privacy and confidentiality. The School is required to comply with privacy and confidentiality requirements regarding student data and health information, including the Family Educational Rights and Privacy Act (FERPA) and the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

In addition, the School did not develop a data use agreement as required by Texas Government Code, Section 2054.135 (see text box for more information about data use agreement requirements). That agreement should be distributed to and signed by employees who handle sensitive information, such as financial, medical, personnel, or student 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 Web site.

Sources: The Texas Government Code and DIR.

Data Classification and Asset Inventory. The School did not define and document its information classification categories or classify its data, as required by Title 1, Texas Administrative Code, Section 202.24 (1 TAC 202.24) (see text box for more information about data classification requirements). In addition, the School did not document a prioritization of its information technology (IT) assets as described by DIR's *Texas Cybersecurity Framework Control Objectives and Definitions*. Data classification and IT asset prioritization are necessary for the School 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.

Data Classification Requirements

According to 1 TAC 202.24(b)(1), state agencies must define all information classification categories, except for the Confidential Information category, and establish controls for each.

DIR has a *Data Classification Guide* and *Data Classification Template* available on its Web site.

Sources: The Texas Administrative Code and DIR.

In addition, the School's inventory controls were not suitably designed to ensure the completeness and accuracy of the School's IT asset inventory. For example:

- The School's inventory policies and procedures did not provide detailed instructions for tracking inventory or for performing the School's annual inventory.

- The School lacked a centralized and complete list of its IT assets that was routinely maintained. Although the School had device management software that tracked its laptops and tablets, that software did not track the School's other IT assets, such as its servers, network devices, and software. As a result, the School did not comply with requirements in Texas Government Code, Section 2054.068, to submit information about its IT infrastructure to DIR, including an IT asset inventory that listed the cloud services it used (see text box for more information about IT reporting requirements).

IT Infrastructure Reporting Requirements

Texas Government Code, Section 2054.068, requires state agencies to report to DIR information about the condition of their information technology infrastructure, including (1) their information security program; (2) an inventory of servers, mainframes, cloud services, and other information technology equipment; and (3) identification of vendors that operate and manage their information technology infrastructure.

Source: The Texas Government Code.

Risk Assessment and Management. The School did not perform and document a risk assessment of information and information systems as required by Title 1, Texas Administrative Code, Section 202.25 (1 TAC 202.25) (see text box for information about risk assessment requirements). In addition, the School's lack of data classification and IT asset prioritization impeded the School's ability to perform an adequate risk assessment and establish its risk management strategy. As a result, the School did not implement an appropriate risk management strategy to respond to its information security risks, including the identification and implementation of necessary security control activities. For example, it did not catalog and evaluate its information security control activities as required by DIR's minimum standards.

Risk Assessment Requirements

According to 1 TAC 202.25, state agencies must perform and document a risk assessment of their information and information systems. At a minimum, the risk assessment should document the ranking of inherent risks and the frequency of future risk assessments. In addition, the information security officer, in coordination with information owners, is responsible for risk management decisions for systems identified with a low or moderate residual risk, and the agency head is responsible for systems identified as having a high residual risk.

DIR's Web-based governance, risk, and compliance tool—Statewide Portal for Enterprise Cybersecurity Threat, Risk and Incident Management (SPECTRIM)—includes a risk assessment tool that state agencies can use.

Sources: The Texas Administrative Code and DIR.

Governance Structure and Oversight. The School should make improvements to ensure that its governance structure, which includes the School's governing board, executive management, and information security officer (ISO), has adequate oversight of the School's information security program. For example, although Title 1, Texas Administrative Code, Chapter 202 (1 TAC 202), specifies the responsibilities of an ISO, the School had not adequately defined and documented the duties and authorities of its ISO position, such as the development and maintenance of the School's information security policies, standards, and procedures.

Awareness and Training Program. The School should ensure that all personnel, including the governing board, executive management, the ISO, information owners, and system users, have sufficient training on cybersecurity risks and their responsibilities as required by DIR's information security standards. Specifically:

- Adequate training at the governance level is necessary for proper prioritization, oversight, and monitoring of the School's information security program.

- Personnel responsible for carrying out information security activities, such as IT department staff (including the ISO), did not have sufficient role-based security training. Additional training is necessary to increase their understanding of the requirements of 1 TAC 202 and DIR's *Security Control Standards Catalog*.

- Although the School had annual cybersecurity training as a strategic goal in its *Agency Strategic Plan 2017-2021*, it had not implemented a security and privacy awareness training program for all users as required by DIR's *Security Control Standards Catalog*. A training program would help ensure that all employees are aware of cybersecurity threats and privacy risks.

Recommendations

The School should increase its oversight of its information security program to ensure compliance with statute and DIR's minimum standards, including:

- Establishing a framework to develop its information security policies, standards, and procedures, including implementing a process to periodically review, approve, and update those documents.
- Developing a data use agreement as required by Texas Government Code, Section 2054.135.
- Defining and documenting its information classification categories and performing and documenting its data classification.
- Performing and documenting an IT asset prioritization and strengthening controls over its IT asset inventory process.
- Performing and documenting a risk assessment and establishing and documenting a risk management strategy that includes its evaluation of security control activities.
- Defining and documenting the duties and authorities of its ISO.
- Implementing a training program for all personnel, including role-based security training and security awareness and privacy training.

Management's Response

- ***TSD submitted an Information Security Plan to DIR in October of 2018, as required.*** *The school will implement the recommendation to strengthen our information security policies, standards and procedures and will periodically review, approve and update these documents.*
- ***The School Has Developed a Data Use Agreement*** *in the form of a TSD Administrative Regulation. This document will be distributed to ALL TSD staff and shared at all (NEOs) - New Employee Orientations, throughout the school year so that every employee is aware of and acknowledges this regulation.*
- ***Data Classification Definitions and Documentation –*** *We have reviewed DIRs Data Classification Guide and Template and have developed a plan to evaluate the data classifications at TSD. The ISO will send the definitions to each administrator and or program supervisor to determine the types of data in each system to verify they are classified correctly.*

- ***IT Asset Prioritization and IT Asset Inventory*** *–TSD reports our IT assets through our Biennial Operating Plan (BOP) Life Cycle inventory and in our Information Technology Detail (ITD) report. Through this audit process we have become aware of additional requirements for reporting IT assets. TSD's ISO and IRM will review the DIR IT Infrastructure Reporting Requirements to update our policies and procedures with detailed instructions for performing the annual inventory and prioritizing our IT assets.*

- ***Risk Assessment and Management Strategy*** *– Once the School has completed our IT asset prioritization and inventory we will begin our risk assessment to assist us in developing a risk management strategy per the requirements of TAC 202.25.*

- ***Defining and documenting the duties and authorities of its ISO.*** *– The School's former ISO of 15+ years retired from the agency in of Aug 2018 and subsequently passed away. We recently appointed a new ISO effective October 1, 2018. This staff member is also the school's Systems Analyst and is responsible for TSD's network infrastructure, all TSD servers, the wireless network, back-up systems, Cloud storage AND also the newly assigned responsibilities as the agency's ISO. The ISO is currently studying for Computing Technology Industry Association (CompTIA) Security+ certification and will become certified. This will help the agency to define and document the duties and authorities of TSD's ISO.*

- ***Implementing a training program for all personnel, including role-based security training and security awareness and privacy training.*** *– Subsequent to our new ISO receiving training for his role, we will work on training for all personnel related to security awareness and privacy training. Topics to be covered in the trainings include:*

    1) *Threats, Attacks, and Vulnerabilities*
    2) *Identity and Access Management*
    3) *Architecture and Design and*
    4) *Risk Management*

Chapter 1-B

The School Should Strengthen Its Processes and Controls to Ensure That External Service Providers Meet Its Information Security Requirements

Chapter 1-B Rating:

High [2]

The School relies on external service providers for its IT needs, including cloud-based services and products. However, it has not developed related policies and procedures to ensure that those providers meet the School's information security requirements. Those policies and procedures should include (1) an evaluation of information security during the planning process to acquire and implement services and products and (2) monitoring of providers' compliance with security requirements.

As discussed in Chapter 1-A, the School did not adequately define its information security policies and procedures, which impaired its ability to ensure that providers met its security requirements. Based on auditors' review of planning documentation and discussion with School personnel, the School's planning process for its acquisition of services and products provided by external service providers did not include an evaluation of whether those providers could meet the School's information security requirements. Having documented policies and procedures for external service providers could help the School ensure consistency in its acquisition, implementation, and monitoring of external services and products.

Google G Suite for Education

One example of the School's use of an external service provider's services and products is its implementation of Google G Suite for Education (G Suite). G Suite includes several Web-based applications such as email (Gmail) and cloud storage (Google Drive). G Suite is offered at no cost to the School, so neither party signs a contract. Instead, the School must agree to Google's terms in its online agreement. Because the School had not adequately evaluated whether Google could meet its information security requirements, it was not aware that Google restricts the use of G Suite for entities required to comply with HIPAA. Although the terms in the online agreement indicated Google would comply with FERPA requirements, the agreement stated that the School was responsible for compliance with HIPAA. The online agreement also required the School to enter into an additional HIPAA Business Associate Agreement with Google if it planned to store or transmit protected health information using G Suite services, and the School did not enter into that additional agreement.

[2] The risk related to the issues discussed in Chapter 1-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 School asserted that it does not store or transmit protected health information using G Suite services. However, as discussed in Chapter 1-A, the School did not perform a data classification, which would help the School (1) identify and maintain its protected health information and (2) assign the necessary levels of protection, such as developing and implementing a policy restricting the usage of G Suite for users handling protected health information.

Recommendations

The School should:

- Develop and document policies and procedures to ensure that external service providers meet the School's information security needs, including procedures to evaluate information security during the planning process and to monitor providers' compliance with its information security requirements.
- Develop and document a policy regarding the storage and transmission of protected health information.

Management's Response

- *TSD will continue our current practice of ensuring that external service providers meet the School's information security requirements. The ISO will also verify that all external/cloud providers meet the information security requirements of the school. Future external service providers will need to be reviewed by the ISO* **before** *new purchases are made to ensure they are compliant with DIR security policies and standards.*
- *The school does NOT transmit PHI (personal health information) using G Suite services. The school will develop an Administrative Regulation regarding the storage and transmission of PHI. Additionally, the School has recently purchased a new software program called SNAP Health Center which maintains full FERPA and HIPAA compliance, ensuring that data remains secure and protected at all times.*

Chapter 2

The School Should Implement or Improve Processes and Controls to Ensure That It Safeguards Its Information Assets

The School should implement or improve certain processes and controls to ensure that its information assets are protected against unauthorized or inappropriate access, use, and modification. While the School had controls to enforce and monitor its system configurations, it did not fully establish and document those configurations, and it did not have a process in place to manage system development and changes.

In addition, the School should strengthen controls to ensure that it restricts access to its data appropriately. Auditors identified significant weaknesses in the School's controls over access to its information systems.

Chapter 2-A

The School Should Establish and Document Its System Configurations and Its Processes for System Development and Change Management

Chapter 2-A Rating:

Medium [3]

The School did not adequately establish and document its system configurations, and it did not develop and implement processes, policies, or procedures to manage development of and changes to its information systems as required by DIR's minimum security standards.

System Configurations. Although the School had controls, such as its device management software, in place to enforce and monitor system configuration settings, it did not fully establish or document its baseline configurations for its information systems and system components, such as its servers, laptops, tablets, and network devices. According to the National Institute of Standards and Technology, baseline configurations are documented, reviewed, and agreed-upon sets of specifications for information systems, and those specifications include information about system components, such as standard software packages, patch information, and configuration settings (including those for security).[4] Per DIR's *Texas Cybersecurity Framework Control Objectives and Definitions*, an entity should base its configurations on its organizational risk management strategy.

System Development and Change Management. The School did not implement documented system development life cycle processes, policies, or

[3] The risk related to the issues discussed in Chapter 2-A is rated as Medium because the 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 and reduce risks to a more desirable level.

[4] The National Institute of Standards and Technology's *Special Publication 800-53, Revision 4: Security and Privacy Controls for Federal Information Systems and Organizations*.

procedures to manage the development of new information systems. In addition, the School did not develop, document, and implement change management processes, policies, or procedures to track and manage system changes, including patches. Those procedures should include a documented review and approval of system changes prior to implementation. Inadequate change management processes can affect data integrity, such as unintentional loss or alteration of data, and system availability, such as unplanned system downtime.

Recommendations

The School should:

- Establish and document its baseline configurations for its information systems and system components.
- Develop and document its processes, policies, and procedures to manage the development of new information systems and changes to existing systems.

Management's Response

- *The School will review this recommendation and establish baseline configurations and system components based on the completion and findings in our risk management assessment. TSD has an ongoing annual hardware replacement schedule, with a 4 to 5-year life cycle, so it is complex to have baseline configurations established as our hardware and software changes annually based on capital budget appropriations.*
- *The School will document our processes, policies, and procedures to manage the development of new systems and changes to existing systems.*

Chapter 2-B

The School Should Strengthen Access Controls Over Its Information Systems

Chapter 2-B Rating:

High [5]

Auditors identified significant weaknesses in the School's controls over access to its information systems. To minimize security risks, auditors communicated details about the identified weaknesses related to access separately to the School in writing.

Pursuant to Standard 7.41 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 provisions of Texas Government Code, Section 552.139, the omitted information is also exempt from the requirements of the Texas Public Information Act.

Management's Response

The School has already taken actions to strengthen access controls over its Information Systems and will continue to enhance our security controls.

[5] The risk related to the issues discussed in Chapter 2-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.

Chapter 3

Although the School Implemented Network and Physical Security Controls, It Should Strengthen Certain Controls Over Its Incident Detection, Response, and Recovery Planning

Chapter 3 Rating:

Medium [6]

Auditors assessed controls over the School's network and physical security and its incident detection, response, and recovery planning. While the School had some security controls in place, it should strengthen certain controls in those areas. To minimize security risks, auditors communicated details about the identified weaknesses separately to the School in writing.

Pursuant to Standard 7.41 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 provisions of Texas Government Code, Section 552.139, the omitted information is also exempt from the requirements of the Texas Public Information Act.

Management's Response

The School will continue to strengthen, improve and document its security procedures and processes.

[6] The risk related to the issues discussed in Chapter 3 is rated as Medium because the 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 and reduce risks to a more desirable level.

Appendices

Appendix 1

Objective, Scope, and Methodology

Objective

The objective of this audit was to determine whether the School for the Deaf (School) has implemented information system 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 system security standards and controls over the School's significant information technology systems and assets from September 1, 2017, through December 31, 2018.

Methodology

The audit methodology included gaining an understanding of the School'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 School to review user access for significant information technology systems. To determine whether that data was valid and complete, auditors (1) observed the School's extraction of user access data sets, (2) analyzed the data, and (3) reviewed user access. Auditors determined that the data was sufficiently reliable for the purpose of this audit.

Sampling Methodology

Auditors selected a risk-based sample of the School's database applications for user access testing. Specifically, auditors selected four database applications containing personally identifiable information. The sample

database applications were generally not representative of the population; therefore, it would not be appropriate to project those test results to the population.

Information collected and reviewed included the following:

- The School's policies and procedures.
- Job descriptions for the School's information technology department staff.
- Supporting documentation related to the School's information security plan and standards.
- Supporting documentation related to controls over the School's significant information technology systems.
- Supporting documentation related to the School's tracking of its information technology assets.
- User access data for significant information technology systems.
- Password parameters for significant information technology systems.
- The School's *Agency Strategic Plan 2017-2021* and Board meeting minutes.
- Contract documentation for significant information technology systems.

Procedures and tests conducted included the following:

- Interviewed the School's management and staff.
- Reviewed policies, procedures, and supporting documentation and observed controls over the School's significant information technology systems and assets for compliance with statute and DIR's information security standards.
- Reviewed the School's *Agency Strategic Plan 2017-2021*, Board meeting minutes, job descriptions for the information technology staff, and training requirements to determine the key responsibilities and levels of oversight in managing information security risks for the information technology department staff, executive management, and the governing board at the School.
- Reviewed contract documentation for significant information technology systems to determine whether the School implemented controls to

ensure that external service providers (including cloud technology providers) met information security requirements.

- Performed a walkthrough of the School's server room to determine whether physical security controls were in place.
- Tested logical access to the School's significant information technology systems to determine whether system access permissions for users were appropriate.
- Tested 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*.
- NIST's *Special Publication 800-53, Revision 4: Security and Privacy Controls for Federal Information Systems and Organizations*.
- NIST's *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1.
- The Health Insurance Portability and Accountability Act of 1996 (HIPAA).
- The Family Educational Rights and Privacy Act (FERPA).
- The School's policies and procedures.

Project Information

Audit fieldwork was conducted from October 2018 through January 2019. 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:

- Sonya Tao, CFE (Project Manager)

- Rachel Goldman, CPA (Assistant Project Manager)
- Benjamin Hikida, MAcy
- Joe Kozak, CISA, CPA
- Michelle Rodriguez, CFE
- Dennis Ray Bushnell, CPA (Quality Control Reviewer)
- George D. Eure, CPA (Quality Control Reviewer)
- Michael A. Simon, MBA, CGAP (Audit Manager)

Appendix 2

Issue Rating Classifications and Descriptions

Auditors used professional judgement 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 2 provides a description of the issue ratings presented in this report.

Table 2

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

The School's Response to the Overall Conclusion

The School for the Deaf (School) provided the following management response to the Overall Conclusion section of this report.

> *Texas School for the Deaf (TSD) has responded to the specific recommendations in the Cybersecurity Audit Report. We would like to also respond to the Overall Conclusion that states:*
>
> The School for the Deaf (School) should strengthen its information security program to meet statutory requirements and the Department of Information Resources' (DIR) information security standards.
>
> - *The School will continue to enhance and implement its information security program as required. Texas School for the Deaf (TSD) submitted its Information Security Plan to DIR in October 2018. Though we were never notified of any non-compliance, we agree with the auditor's overall finding that we need to strengthen our information security program at TSD.*
> - *Cybersecurity responsibilities at TSD are an "add on" to the job description of our Systems Analyst. There is no department with multiple staff as one would routinely find in state agencies. Additionally, TSD with its dual role as a state agency that functions more similarly to an independent school district, often presents unique challenges in applying state agency standards and policies. Currently, Senator Nelson is sponsoring a bill on cybersecurity for school districts, which we hope will be more relevant for us.*
> - *We are appreciative of the audit recommendations and are committed to strengthening our cybersecurity efforts at TSD.*

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 John Zerwas, House Appropriations Committee
The Honorable Dustin Burrows, House Ways and Means Committee

Office of the Governor

The Honorable Greg Abbott, Governor

School for the Deaf

Members of the School for the Deaf Governing Board

- Mr. Eric Hogue, President
- Dr. Shawn Saladin, Vice President
- Ms. Susan Ridley, Secretary
- Ms. Sha Cowan
- Mr. Ryan Hutchison
- Mr. Tyran Lee
- Ms. Angie Wolf
- Mr. David Saunders

Ms. Claire Bugen, Superintendent