INTERNAL AUDIT OF THE INFORMATION SYSTEMS - SECURITY

As of July 27, 2018

AT THE

TEXAS ANIMAL HEALTH COMMISSION

(REPORT NO: TAHC 018-003)

MONDAY RUFUS & CO., P.C.

CERTIFIED PUBLIC ACCOUNTANTS AND ADVISORS

MONDAY RUFUS & CO., P.C.
Certified Public Accountants & Advisors

Audit Committee
And Commissioners
Texas Animal Health Commission
Austin, Texas

We have conducted an internal audit (audit) of the Information Systems - Security at the Texas Animal Health Commission (Commission) as of July 27, 2018. The results of our audit disclosed that the Commission has procedures and controls in place related to the Information Systems - Security. We noted an opportunity for enhancing the processes and controls in place.

We appreciate the courtesy and cooperation the management of the commission showed during the course of the engagement.

Monday Rufus & Co., P.C.

July 27, 2018
Austin, Texas

(512) 380-0799 7701 North Lamar Blvd., Ste 417 Austin, Texas 78752 Fax (512) 380-0797

TABLE OF CONTENTS

Executive Summary

Information Security is a continual process of protecting information resources. The Texas state government considers information resources as vital strategic assets. Protecting information resources includes data, information hardware/software, and the network as advances in computer technology occur. There are always risks and vulnerabilities that impact new and legacy information systems. Some vital information may be in non-electronic or in paper form that still requires protective measures for insuring security. Security is everyone's responsibility and an effective information security program relies on a continual training and education of employees about threats with an emphasis in best security practices.

Legislation relating to information technology is becoming more prolific, with many laws on different issues. These legislative pressures require the implementation of proper security policies and related local access controls. To meet the basic business requirements, a good practice should ensure the integrity of the information stored on its computer systems, preserve the confidentiality of sensitive data, ensure the continued availability of its information systems, and ensure conformity to laws, regulations and standards.

TAHC's Information Resources Department (IR) is responsible for designing and developing automated data collection, processing, and reporting tools. This department strives to provide enhanced technological capability to better serve the Agency and its clients and/or customers. The IR department is comprised of an information resource manager, two network specialists, a systems analyst, and a system support specialist. One of the network specialists also serves as the Information Security Officer.

The IR department's routine responsibilities include maintenance of the local area network and telecommunications system for TAHC's central location and field offices. The IR department is responsible for forecasting and planning the TAHC's technological needs, maintaining and updating the agency's website, hardware and software upgrades, systems development, and information security.

The Department of Information Resources (DIR) Security Control Standards Catalog and the National Institute of Standards and Technology (NIST) 800-53 Publication outline security standards policy, management and staff responsibilities, requirements for managing security risks, requirements for managing physical security, information resources security safeguards, how to manage security incidents; and user security practices, respectively, for state agencies.

Internal Audit Results

TAHC has implemented good controls over security for information systems. However, this system could be strengthened by maintaining a written wireless access policy.

Matters For Further Study

Our audit did not include testing the TAHC's network security through Internet connectivity. The Department of Information Resources (DIR) Security Office conducted a Controlled Penetration Test for the TAHC to assess network security and issued a report dated September 9, 2016.That report noted that while some vulnerabilities were discovered, the systems could not be compromised, and proprietary information was not retrieved. We recommend that the TAHC continue to assess the effectiveness of its security systems on a continuous basis.

Summary of Management's Response

As noted in your report, our access controls are in place and operating effectively. Although we found that access controls are in place and operating effectively.

We have renamed the SSIDs from the default name, and we do not have the Agency's full name included in the SSID network name. We do not authorize any installation of wireless personal networking equipment and we do monitor for such unauthorized installations. We use the WPA2 security standard and does provide encryption. As suggested, we will incorporate these specifications in our written wireless network policy. We should have our wireless policy completed within the next ninety days.

Objectives, Observations, Findings, Recommendations, and Management's Response

The primary objectives of the internal audit were to determine the following:

- Reliability and Integrity of Information
- Compliance with Policies, Procedures, Laws, and regulations
- Efficiency and Effectiveness of operating procedures.
- Safeguarding of assets

RESULTS AND RECOMMENDATIONS

The TAHC has developed an adequate system to ensure that the processes of developing information systems are effective. During our review we noted the following:

Internal Audit Objectives 1 and 2: Reliability and Integrity of Information, and Compliance with Policies and Procedures, Laws, and Regulations

- TAHC has maintained an agency-wide information security program to ensure that policies and procedures are followed
- TAHC has a process in place for addition, change, or deletion of Network access.
- TAHC has a designated Information Security Officer (ISO) who is charged with, among other things, developing and maintaining information security policies and procedures
- Agency's computer users are prompted to change their passwords periodically

Internal Audit Objective 3: Efficiency and Effectiveness

- TAHC grants access to users on a need-to-know basis.
- Passwords are effectively used to control access to TAHC computer resources.

Internal Audit Objectives 4: Safeguarding of Assets

- The Agency has a process in place to restrict access to agency applications with the use of passwords. Passwords are not displayed during logon and contain a combination of letters, numbers, and special characters.
- There is anti-virus software on all computers
- TAHC is up to date with their security patches
- There are adequate controls in place to maintain agency assets
- The computer room is restricted and accessible only to authorized personnel through the use of a key pad.
- The Agency has a documented Information Security policy that defines the responsibilities of user and access is monitored.
- There is a control that ensures transmissions over networks and remove access are protected through the use of VPN and/or password protection.
- There is uninterriptible power supply (UPS) in case of loss of electricity, fire extinguishers, and smoke detectors.
- Mission critical data is backed up on a scheduled basis and stored at a contract offsite location.

However, we identified some conditions that could enhance the established controls and minimize the following risks identified:

Maintain a written policy for the Agency's Wireless Access

Although we found that access controls are in place and operating effectively, however; we noted that some controls relating to the wireless access are not documented.

The TAHC does not have a written policy for their wireless network. According to the Security Control Standards Catalog (AC-18) and NIST Special Publication 800-53 (AC-18), it states that "the wireless policy shall address the following topic areas:

1. Wireless Local Area Networks. Ensure that Service Set Identifiers (SSID) values are changed from the manufacturer default setting. Some networks should not include organizational or location information in the SSID. Additional equipment configuration recommendations are included in the Wireless Security Guidelines.
2. Types of information that may be transmitted via wireless networks and devices with or without encryption including mission critical information or sensitive personal information.

3. Prohibit and periodically monitor any unauthorized installation or use of Wireless Personal Area Networks on state organizational IT systems by individuals without the approval of the state organization information resources manager".

Without the written policy, it will be difficult to determine if unauthorized access ports have been deployed and that approved protections are in place and working.

Recommendation:

We recommend that the agency should maintain a written policy for the wireless access to ensure that proper authorization process is delineated.

Management's Response

As noted in your report, our access controls are in place and operating effectively. Although we found that access controls are in place and operating effectively.

We have renamed the SSIDs from the default name, and we do not have the Agency's full name included in the SSID network name. We do not authorize any installation of wireless personal networking equipment and we do monitor for such unauthorized installations. We use the WPA2 security standard and does provide encryption. As suggested, we will incorporate these specifications in our written wireless network policy. We should have our wireless policy completed within the next ninety days.

Appendix 1

Objective and Scope

Objective

The primary objectives of the internal audit were to determine the following:

- Reliability and Integrity of Information
- Compliance with Policies, Procedures, Laws, and regulations
- Efficiency and Effectiveness of operating procedures.
- Safeguarding of assets

Scope

Our scope included reviewing Texas Administrative Code, Chapter TAC 202.21. We interviewed the appropriate staff of the TAHC, reviewed the TAHC's policies and procedures, tested for compliance with these operating policies and procedures, and reviewed other pertinent reports and documentation.

Methodology

Our procedures included collecting information and documentation; performing selected test and other procedures; analyzing and evaluating the result of the tests; reviewing operating procedures, laws, and regulations, conducting interviews with the appropriate staff of the Commission, testing for compliance with policies, procedures, and laws, and review of other pertinent reports and documentation.

Information collected and reviewed included the following:

- Interviewed the IR Division staff to obtain an understanding of the activities, processes, and controls in place related to information technology/project development.
- Texas Department of Information Resources.
- Obtained and reviewed the Texas Administrative Code related to Information Resources
- Tested for compliance with laws and regulations
- Reviewed other pertinent reports and documents

Criteria Used included the following:

- Texas Administrative Code, Chapter TAC 202.21
- Texas Government Code, Chapter 2054
- Review of other pertinent reports and documents

Other Information

Our internal audit was conducted 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 internal audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our internal audit objectives. Our internal audit also conforms with the Institute of Internal Auditor's (IIA) *International Standards for the Professional Practice of Internal Auditing.*

Appendix 2

Background

In 1893, the agency was created to combat the fever tick that plagued the Texas cattle industry. Since then, the Texas Animal Health Commission (Commission) and the United States Department of Agriculture (USDA) have worked cooperatively with livestock producers on animal health issues. In recent years, the agency's primary objectives have been to control and eradicate livestock diseases, such as: Brucellosis in cattle and swine; tuberculosis in cattle; goats and cervidae; hog cholera in swine; pseudorabies in swine; scabies in cattle and sheep; Venezuelan equine encephalomyelitis (VEE); and equine infectious anemia (EIA) in horses.

The Commission's enabling statutes are in Chapters 161 through 168 of the Texas Agriculture Code, Vernon's Annotated Texas Statutes. The Commission is vested with the responsibility of protecting all livestock, domestic animals, and domestic fowl from diseases stated in the statute, or recognized as maladies by the veterinary profession. The Commission is authorized to act to eradicate or control any disease or transmission of any disease that affects livestock, exotic livestock, domestic animals, domestic fowl, exotic fowl, or canines, regardless of whether or not the disease is communicable. In order to carry out these duties and responsibilities, the Commission is authorized to control the sale and distribution of all veterinary biologics, except rabies vaccine; regulate the entry of livestock, domestic animals, and domestic fowl into the state; and control the movement of livestock.

To carry out its mission, the Commission is supported by the veterinary community, competent laboratory system and epidemiology activities which oversee the diagnosis of diseases, and assures appropriate tracing of the movement of exposed and infected animals to determine the origin of infection and minimize the transmission of disease.

The Commission is composed of thirteen members who are appointed by the Governor with the advice and consent of the Senate. The Governor designates the Chair.

The Commissioners appoint an Executive Director who supervises the Commission's activities. The Commission's operating budget is prepared and approved by the Commissioners on an annual basis, whereas the State legislative appropriation request is determined every two years. Both the budget and appropriations are reviewed and approved by the State Legislature.

The Commission is funded by a combination of state general revenue funds, federal funds from the U.S. Department of Agriculture (USDA), and fee-based revenue. For fiscal year 2017 the Commission has an authorized workforce of 185.2 full-time equivalent employees (FTEs). The Commission's staff is comprised of field inspectors, veterinarians, veterinary epidemiologists, laboratory personnel, emergency management planners, field investigators, and administrative staff.

Appendix 3

Report Distribution

As required by Gov't Code 2102.0091 copies of this report should be filed with the following:

Governor's Office of Budget and Planning
Attn: Sarah Hicks
Phone: (512) 463-1778
Budgetandpolicyreports@governor.state.tx.us

Legislative Budget Board
Attn: Julie Ivie
Phone: (512) 463-1200
Audit@lbb.state.tx.us

State Auditor's Office
Attn: Internal Audit Coordinator
Phone: (512) 936-9500
iacoordinator@sao.state.tx.us

Sunset Advisory Commission
Attn: Ken Levine
Phone: (512) 463-1300
sunset@sunset.state.tx.us

Texas Animal Health Commission
Coleman H. Locke, Chairman
Joseph G. "Joe" Osterkamp
William Edmiston, Jr., D.V.M
Jim Eggleston
Ken Jordan
Wendee C. Langdon, Ph.D.
Joe L. Leathers
Thomas E. Oates
Keith M. Staggs
Leo D. Vermedahl, Ph.D.
Mike Vickers, D.V.M.
Eric D. White
Barret J. Klein

Texas Animal Health Commission Management
Andy Schwartz, D.V.M., Executive Director