Network Perimeter Security - Cybersecurity

Audit Report #21-105

January 28, 2021

The University of Texas at El Paso

Office of Auditing and Consulting

”Committed to Service, Independence and Quality”

The University of Texas at El Paso
Office of Auditing and Consulting Services

500 West University Ave.
El Paso, Texas 79968
915-747-5191
WWW.UTEP.EDU

January 28, 2021

Dr. Heather Wilson
President, The University of Texas at El Paso
Administration Building, Suite 500
El Paso, Texas 79968

Dear Dr. Wilson:

The Office of Auditing and Consulting Services has completed a limited scope audit of Network Perimeter Security-Cybersecurity. During the audit, we identified opportunities for improvement and offered the corresponding recommendations in a separate management letter. We intend the recommendations will assist in strengthening controls and help ensure the achievement of the University's mission, goals and objectives.

We appreciate the cooperation and assistance provided by the Telecommunication Infrastructure, Enterprise Computing, and Information Security staff during our audit.

Sincerely,

Lori Wertz

Lori Wertz
Chief Audit Executive

Report Distribution:

University of Texas at El Paso:
Ms. Andrea Cortinas, Vice President and Chief of Staff
Mr. Luis Hernandez, Vice President for Information Resources
Mr. Lethick Leon Cruz, Assistant Vice President, Telecommunication Infrastructure
Mr. Gerard Cochrane, Chief Information Security Officer
Ms. Mary Solis, Director and Chief Compliance and Ethics Officer

University of Texas System (UT System):
System Audit Office

External:
Governor's Office of Budget, Planning and Policy
Legislative Budget Board
Internal Audit Coordinator, State Auditor's Office

Audit Committee Members:
Mr. Joe Saucedo
Mr. Fernando Ortega
Mr. Mark McGurk
Dr. John Wiebe
Dr. Giorgio Gotti
Mr. Daniel Garcia
Ms. Guadalupe Gomez

Auditor Assigned to the Audit:
Victoria Morrison

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Office of Auditing and Consulting Services has completed a limited scope audit of Network Perimeter Security-Cybersecurity to determine adherence to State and University security controls and standards. Due to the confidential nature of the audit, we issued a separate management letter to the Telecommunication Infrastructure Department, which details specific findings and recommendations. These confidential results are exempt from the Texas Public Information Act under Texas Government Code §552.139.

See "Audit Results" section for a table with the issues identified during the audit.

BACKGROUND

A network is a means of connecting two or more computers, servers, network components, peripherals, etc. for the purpose of sharing information between users. Network components are vital to the overall network architecture as they include both hardware and software. Proper network maintenance and controlled access (both physical and logical) to network components keep an organization's network running and protected against downtime and/or cybersecurity threats.

According to the Cybersecurity and Infrastructure Security Agency (CISA), "*Network infrastructure devices are often easy targets for attackers. Once installed, many network devices are not maintained at the same security level as general-purpose desktops and servers.*" Currently, the University maintains over 1,800 network/Wi-Fi devices.

The University's network is mission critical as faculty, staff, and students rely on it daily for their information resources needs. Therefore, we focused the audit to assess the University's network components concerning network maintenance and logical/physical access control.

AUDIT OBJECTIVES

Our objective for the audit was to assess network components to ensure they provide protections to the University's network in the areas of a) network maintenance and b) logical and physical access control.

SCOPE AND METHODOLOGY

The scope of the audit was limited to network components, excluding firewalls, from September 1, 2019 to November 11, 2020. We did not include firewalls as they were in the process of being replaced during the audit.

We conducted the audit in accordance with the *International Standards for the Professional Practice of Internal Auditing* and the authoritative guidelines of the International Professional Practice Framework issued by the Institute of Internal Auditors.

The criteria and standards used were:

- Texas Administrative Code, Title 1, Part 10, Chapter 202, Subchapter C. §202.72 - Staff Responsibilities and §202.76 - Security Control Standards Catalog
- Texas Department of Information Resource-Security Control Standards Catalog Version 1.3 (TAC 202-76)
- UT System Policy (UTS 165) Information Resources Use and Security Policy and Standards
- UTEP ISO Information Resources Use and Security Policy and Standards

Our audit procedures included:

- interviewing and requesting information from key personnel,
- reviewing applicable laws, regulations, policies, and procedures,
- reviewing business standards for network maintenance,
- verifying the existence of appropriate procedures and policies, and
- limited testing where appropriate

AUDIT RESULTS

Network Areas Covered	Number of Findings* **
Network Components Maintenance	5
Access to Network Components	3

* Due to the confidential nature of the audit, we issued a separate management letter to Telecommunication Infrastructure, which details specific findings and recommendations.

** Telecommunication Infrastructure has implemented corrective actions to address two of these findings. Also, one additional finding was partially implemented. These corrective measures have been validated by the Office of Auditing and Consulting Services.

CONCLUSION

Based on the results of audit procedures performed, we conclude Telecommunication Infrastructure can strengthen existing security controls by implementing the recommendations included in the separate management letter, which contains confidential results exempt from the Texas Public Information Act under Texas Government Code §552.139.

We appreciate the cooperation and assistance provided by the Telecommunication Infrastructure, Enterprise Computing, and Information Security Office staff during our audit.