Critical Security Updates-Cybersecurity

Audit Report # 20-100

April 29, 2020

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

April 29, 2020

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 Critical Security Updates-Cybersecurity. During the audit, we identified opportunities for improvement and offered the corresponding recommendations in a separate management letter. The recommendations are intended to assist the department in strengthening controls and help ensure that the University's mission, goals and objectives are achieved.

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

Sincerely,

Lori Wertz

Lori Wertz
Chief Audit Executive

Report Distribution:

University of Texas at El Paso:
Mr. Richard Adauto III, Chief of Staff
Ms. Guadalupe Valencia-Skanes, Interim Vice President for Information Resources
Mr. Luis Hernandez, Assistant Vice President, Enterprise Computing
Mr. Gerard Cochrane, Chief Information Security Officer
Mr. Lethick Leon Cruz, Assistant Director, System Support, Enterprise Computing
Ms. Rosa Valenzuela, Manager, System Support, Enterprise Computing
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 R. Saucedo
Mr. Daniel Garcia
Dr. Giorgio Gotti
Mr. Mark McGurk
Mr. Fernando Ortega
Dr. John Wiebe

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 Critical Security Updates-Cybersecurity to determine adherence to State and The University of Texas at El Paso (UTEP) security controls and standards. Due to the confidential nature of the audit, we issued a separate management letter to Enterprise Computing, 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

Mission critical systems are those systems that are essential to UTEP achieving its mission; if they fail or suffer from interruptions, it could have a significant impact on UTEP's daily operations. It is important that these systems be available to UTEP personnel and students and, proper security safeguards be in place.

There are several methods for protecting servers that host mission critical systems from cyber security threats. One of the most effective controls to minimize these types of threats is to keep servers up-to-date on the latest security patches (i.e. patch management).

Patch management is the process of acquiring, testing, and applying patches provided by vendors in order to fix flaws and exploitable vulnerabilities in the software or firmware code found in the servers. "*According to the Center for Internet Security (CIS) Controls, National Institute of Standards and Technology (NIST)*, and other security guidelines, patch management is imperative to achieve a more cyber-secure organization. In fact, patch management has been identified by the Australian Defense Signals Directorate as one of the four controls that reduced intrusions by 85 percent*" - (CIS).

State and UTEP regulations and policies allow for exceptions to security controls (including patch management) if they are documented, justified, and approved in collaboration with the Chief Information Security Officer.

While some mission critical systems are hosted in servers maintained by the Enterprise Computing Department, others, like PeopleSoft and Blackboard, are hosted and maintained outside of UTEP. This audit focuses on the servers hosting mission critical systems maintained by the Enterprise Computing Department.

As part of our cybersecurity assurance, we are conducting this patch management audit of critical security updates.

**Note: Texas Administrative Code, Title 1, Part 10, Chapter 202, Subchapter C. §202.76 - Security Control Standards Catalog, Texas DIR Security Control Standards Catalog Version 1.3, aligns with NIST controls*

AUDIT OBJECTIVES

The objective of the audit is to ensure operating systems on servers running mission critical systems have been patched effectively to address vulnerabilities.

SCOPE AND METHODOLOGY

The scope of the audit is limited for the period of September 1, 2018 to January 29, 2020.

The audit will be conducted 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:

- 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
- UTEP ISO Policies Minimum Security Standards for Systems
- UTEP ISO Policies Change Management Guidelines
- UTEP ISO Policies Incident Response Plan

Audit procedures will include:

- interviewing and requesting information from key personnel,
- reviewing applicable laws, regulations, policies and procedures,
- verifying the existence of standard operating procedures and policies, and
- limited testing where appropriate.

RANKING CRITERIA

All findings in this report are ranked based on an assessment of applicable qualitative, operational control and quantitative risk factors, as well as the probability of a negative outcome occurring if the risk is not adequately mitigated. The criteria for the rankings are as follows:

Priority – An issue identified by an internal audit that, if not addressed timely, could directly impact achievement of a strategic or important operational objective of a UT institution or the UT System as a whole.

High – A finding identified by internal audit that is considered to have a medium to high probability of adverse effects to the UT institution either as a whole or to a significant college/school/unit level.

Medium – A finding identified by internal audit that is considered to have a low to medium probability of adverse effects to the UT institution either as a whole or to a college/school/unit level.

Low – A finding identified by internal audit that is considered to have minimal probability of adverse effects to the UT institution either as a whole or to a college/school/unit level.

AUDIT RESULTS

Security Controls and Standards	Number of Observations*
Inventory of mission critical systems and servers	0
Review patch management for the operating system(s) of mission critical servers	3
Security safeguards of server(s) hosting patch management process	1

* Due to the confidential nature of the audit, we issued a separate management letter to Enterprise Computing which details specific observations and recommendations. Enterprise Computing has implemented corrective actions to address one of the three observations; these corrective measures have been validated by us.

CONCLUSION

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

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