Leslie Wilks Garcia, C.P.A., M.Jur.
First Assistant County Auditor

Errika Perkins, C.P.A., C.I.A.
Chief Assistant County Auditor
Audit Division

1001 Preston, Suite 800
Houston, Texas 77002-1817
(832) 927-4600

Fax (713) 755-8932
Help Line (832) 927-4558

MICHAEL POST, C.P.A., M.B.A.
HARRIS COUNTY AUDITOR

August 27, 2021

Dear David Berry, County Administrator and Shain Carrizal, Senior Director, HRRM:

The Harris County Auditor's Office Audit Division has completed an audit of Cybersecurity Training Compliance. The results of our audit are included in the attached report.

We appreciate the time and attention provided by your team. Please expect an email request to complete our Post Engagement Survey. We look forward to your feedback. If you have any questions, please contact me or Errika Perkins, Chief Assistant, 713-274-5673.

Sincerely,

Michael Post
County Auditor

Report Copies:
District Judges
County Judge Lina Hidalgo
Commissioners:
R. Jack Cagle
Rodney Ellis
Adrian Garcia
Tom Ramsey
Christian Menefee
MG Richard J. Noriega
Ed Gonzalez
Ted Heap
Phil Sandlin
Roberto Treviño

AUDIT REPORT

CYBERSECURITY TRAINING COMPLIANCE

AUGUST 20, 2021

Executive Summary

OVERALL CONCLUSION

Harris County (County) accurately reported the cybersecurity training completion percentage ranges for the reporting groups identified by the Texas Department of Information Resources (DIR) in accordance with Texas Government Code 2054.5191 by the June 15, 2021, deadline. The ranges for the reporting groups are as follows:

Reporting Groups	Range Reported
Harris County	90-99%
9-1-1 Emergency Network	100%
Flood Control District	90-99%
Office of Emergency Management	90-99%
Public Health and Environmental Services	90-99%
Public Library	90-99%
Toll Road Authority	100%

The audit identified some opportunities for improvement for management's consideration.

SCOPE AND OBJECTIVE

Information Systems Audit conducted an audit to determine County's compliance with Texas Government Code (TGC) 2054.5191, Cybersecurity Training Required.

The audit reviewed the period of June 16, 2020, to June 15, 2021.

SUMMARY OF AUDIT ISSUE

The County has not established a consistent and formal methodology for identifying the population of employees required to complete a cybersecurity training program.

This issue, management's action plan, and background information are discussed in more detail on the following pages.

AUDIT ISSUE

ISSUE #1: Identification of Employees Requiring Training

What is the Issue: The methodology for identifying the population of employees required to complete a cybersecurity training program could be improved. This includes using a date earlier than the reporting date for the populations identification (e.g., prior to the reporting deadline), handling of new hires, excluding contractors, and formally documenting exempt employees and elected and appointed officials.

What is Expected: The local government is responsible for establishing the mechanism and timing of this annual training.[1] The local government is expected to complete annual training by June 14 and to certify compliance by June 15 of each year.

In May 2021, House Bill 1118 (HB1118) amended the Texas Government Code (TGC) 2054.5191, to read as follows[2]:

> (a-1) At least once each year, a local government shall:
> (1) identify local government employees and elected and appointed officials who have access to a local government computer system or database and use a computer to perform at least 25 percent of the employee's or official's required duties; and
> (2) require the employees and officials identified under Subdivision (1) to complete a cybersecurity training program certified under Section 2054.519.

TGC 2054.5191 states that access to non-compliant individuals may be denied, as follows:

> (a-2) The governing body of a local government or the governing body ’s designee may deny access to the local government ’s computer system or database to an individual described by Subsection (a-1)(1) who the governing body or the governing body ’s designee determines is noncompliant with the requirements of Subsection (a-1)(2).

Why it Matters: Failure to comply with TGC 2054.5191 may result in the County being required to refund the State and becoming ineligible to receive State grants for up to two years, as stated in TGC 772.012:

> (b) To apply for a grant under this chapter, a local government must submit with the grant application a written certification of the local government's compliance with the cybersecurity training required by Section 2054.5191.
>
> (c) On a determination by the criminal justice division established under Section 772.006 that a local government awarded a grant under this chapter has not complied with the cybersecurity training required by Section 2054.5191, the local government shall pay to this state an amount equal to the amount of the grant award. A local government that is the subject of a determination described by this subsection is ineligible for another grant under this chapter until the second anniversary of the date the local government is determined ineligible.

Why it Happened: The County chose to adopt the Texas Department of Information Resources’ (DIR) training deadline of June 14th as the day of record to identify local government employees and elected

[1] https://dir.texas.gov/View-About-DIR/Information-Security/Pages/Content.aspx?id=154#faqs “Each organization should develop internal policies regarding when new employees take their training. If employees take training annually, that complies.”
[2] https://capitol.texas.gov/tlodocs/87R/billtext/html/HB01118F.HTM

and appointed officials to complete a cybersecurity training program. June 14th is the day prior to the required reporting deadline to the State. As a result, the population fluctuated until the reporting deadline creating a compressed schedule for validating the population and the training completion percentages. In addition, the County has not formally documented a procedure for identifying exempt individuals.

What Action(s) are Suggested:

A. Obtain the County Attorney's interpretation of HB1118 and the requirements for the County. This should include the ability to set an earlier date for population identification, the definition of compliance, and whether non-compliant individuals should have their access to County systems suspended.
B. Obtain a revised Commissioner's Court letter designating Human Resources & Risk Management (HRRM) as the designee to deny access to certain employees who have not completed training.
C. Establish a set date for identification of the population required to complete cybersecurity training.
D. Obtain a list of all County employees from HRRM as of the set date. Identify the population required to complete a cybersecurity training by a date early enough that a proper review and resolutions can be obtained before the County is required to report on compliance.
E. Develop a formal process for departments to identify the exempt employees and elected and appointed officials as required by TGC 2054.5191.

MANAGEMENT'S ACTION PLAN

Responsible Party: HRRM Directors (Sakita Douglas and Erika Owens) and Interim Chief Cybersecurity Officer (Dr. Daniel Harrison)

Action Plan: Human Resources & Risk Management (HRRM) and Universal Services (US) will obtain the County Attorney's interpretation of the revised statute HB1118 and prepare a Cybersecurity and Awareness procedure document to be approved by Commissioners Court. This document will outline Cybersecurity training requirements for Harris County employees, including population identification, exemption, and ramifications for non-compliance.

Due Date: October 31, 2021

BACKGROUND

Texas DIR required certification for 7 reporting groups within Harris County. These groups are Harris County, 9-1-1 Emergency Network, Flood Control District, Office of Emergency Management, Public Health and Environmental Services, Public Library, and Toll Road Authority.

Most County departments utilized the training program that was designed and delivered by US Four departments opted to obtain training independent of Universal Services:

Department	Certified Cybersecurity Training Program
Constable Precinct 5	Criminal Justice Information System (CJIS)
Constable Precinct 8	Criminal Justice Information System (CJIS)
Sheriff's Office	Criminal Justice Information System (CJIS)
Toll Road Authority	KnowBe4

HRRM obtained evidence of training from US and the individual departments. HRRM certified on each entity's behalf as authorized by Commissioners Court on February 25, 2020, agenda item 7(a).

ACCOUNTABILITY

We conducted our audit in accordance with the International Standards for the Professional Practice of Internal Auditing ("Standards"). The Standards require that we comply with the Code of Ethics and obtain reasonable assurance that significant risks to the activity are minimized to an acceptable level.

The engagement's scope did not include a detailed inspection of all transactions. There is a risk that fraud or errors were not detected during this engagement. Therefore, the official retains the responsibility for the accuracy and completeness of their financial records, and for ensuring sufficient controls are in place to detect and prevent fraud, errors, or omissions.