FORT WORTH®

INTERNAL AUDIT REPORT

Remote Access Security

January 3, 2023

Audit Staff

David A. Medrano — 1-3-2023
City Auditor — Date

Brian Burkland — 1-3-2023
Assistant City Auditor — Date

Tom Wilson — 1-3-2023
Information Technology Auditor — Date

Executive Summary

This *Remote Access Security* Audit was performed in accordance with the approved schedule of engagements identified in the Department of Internal Audit Fiscal Year 2022 Annual Audit Plan.

As part of the Fiscal Year 2022 Annual Audit Plan, the Department of Internal Audit conducted this Remote Access Security Audit. The IT Solutions Department provides remote access into the City's computer network (Network) for employees, as well as contractors and vendors as needed, who are engaged in official City-related business. Remote access allows authorized users to access the City's Network from any non-City (Offsite) location using an internet connection and City-authorized and installed remote connection software.

Internal Audit staff performed remote access testing to verify the existence of internal controls, and to determine whether those controls are sufficient to minimize the risks associated with unauthorized, remote access into the City's Network. Our testing identified an internal control weakness that allows a user to access the City's Network, using authorized credentials, with a non-authorized device, exposing the City's data and computer resources to potential misuse and heightened susceptibility to cyber-attacks.

Our audit findings are discussed in further detail within the Detailed Audit Findings section of this report.

Table of Contents

FORT WORTH®

Background

A computer network (Network) is commonly considered to be two or more computers that are connected with one another for the purpose of communicating data electronically. Data communication within a Network involves the use of wires, cables, fiber optics, and wi-fi connections to facilitate the transmission of data from one point to another. The City of Fort Worth (CFW) Network is categorized as a wide-area network, because it consists of multiple computers and peripherals located at multiple buildings/sites throughout the City.

Remote access to the CFW Network is managed through authorized user accounts and authorized hardware registered with the IT Solutions Department, and the permissions granted to both. These user accounts and their permissions determine what computer resources and data can be accessed, and govern how and where the access occurs. CFW Network access can occur either within a City facility, or from any Offsite location with an internet connection. Offsite access (i.e. Remote Access) was prominently used by CFW employees during the COVID-19 pandemic.

Audit Objectives

The objectives of the audit were to determine whether the City has internal controls that ensure risks related to Remote Access are minimized, and to evaluate the effectiveness and efficiency by which those controls would provide secure, authorized connectivity between the City's Network and those computer assets through which Remote Access is obtained.

Audit Scope

Citywide, with a review of available data within the test period between October 1, 2020 and June 30, 2022.

Methodology

To achieve the audit objective, the Department of Internal Audit performed the following tests and procedures:

- reviewed CFW Information Technology Security Administrative Regulations;
- interviewed IT Solutions Department personnel;
- reviewed listings of active and authorized CFW user accounts;
- reviewed remote access logs and reports; and
- evaluated internal controls related to Remote Access.

FORT WORTH

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.

Audit Results

Based on our test results, we determined that the IT Solutions Department has taken some commendable measures to ensure Remote Access into the City's network is controlled and monitored. Such measures include a multi-factor authentication process, implemented in October 2020, that provides enhanced security for users connecting remotely to the Network.

However, our testing identified an internal control weakness that allows a user to access the City's Network in an unauthorized manner. This weakness could lead to the potential misuse of City data and computer resources, and heighten the City's susceptibility to cyber-attacks.

The Department of Internal Audit would like to thank the IT Solutions Department for their cooperation and assistance during this audit.

Overall Risk Evaluation

High	Medium	Low
Unauthorized Remote Access to the CFW Network occurred during audit tests and procedures		

FORT WORTH

Detailed Audit Findings

1. Unauthorized Remote Access into the City of Fort Worth (CFW) Network was obtained.

The CFW IT Solutions Department provides two (2) approved methods to enable authorized, secure, Remote Access into the City's Network, and to prevent unauthorized access to and usage of the Network. Both methods require the use of an internet connection and City approved remote connectivity software installed onto an authorized computer to be used for Remote Access. Those methods are as follows:

- Virtual Private Network (VPN) and Multi-Factor Authentication – used by CFW employees/contractors who are remotely accessing the Network with a City-issued computer
- Virtual Desktop Infrastructure (VDI) and VMWare – used by authorized vendors/contractors who remotely access the Network with a personally-owned computer (not City-issued)

The Department of Internal Audit performed tests to verify whether existing internal controls associated with the approved methods are sufficient to mitigate risks associated with unauthorized Remote Access into the City Network. The tests determined that is possible to access the City Network and its resources, using authorized credentials, with a non-authorized device. This issue represents an internal control weakness that, if not timely addressed, could allow individuals to access the City Network and gain unauthorized access to, and the use and control of, City resources and data.

Recommendation 1A: *The Chief Technology Officer should ensure that access to the CFW Network occurs only using approved methods, and that devices not authorized for Remote Access to the CFW Network are prevented from achieving such access.*

Auditee's Response: Concur. As part of the existing strategic plan, IT Solutions will configure and deploy a Network Access Control solution to mitigate this concern as we increase the security of the overall environment.

Target Implementation Date: July 31, 2023

Responsibility: Sallie Trotter, Assistant IT Solutions Director

Applicable Department Head: Kevin Gunn, Chief Technology Officer

Applicable Assistant City Manager: Valerie Washington

Recommendation 1B: *The Chief Technology Officer should ensure that Remote Access logs are monitored on a scheduled basis for unauthorized access, ensure that root causes of unauthorized attempts are identified, and lessons learned incorporated into training in order to minimize similar unauthorized attempts.*

Auditee's Response: Concur. As part of the existing strategic plan, IT Solutions will implement the next level of capabilities within the currently implemented Security Incident and Event Management technology to monitor Remote Access logs. Events or trends in this information will be reviewed regularly and lessons learned will be incorporated into operations and training to mitigate the threats of unauthorized access.

Target Implementation Date: July 31, 2023

Responsibility: Donlen Ruffin, Assistant IT Solutions Director

Applicable Department Head: Kevin Gunn, Chief Technology Officer

Applicable Assistant City Manager: Valerie Washington