CITY AUDITOR'S OFFICE

Wireless Network Security

June 10, 2022

AUDIT NO. 2203

June 10, 2022

Honorable Mayor and Members of the City Council:

Enclosed is the audit report for *Wireless Network Security*, which was included on the Council-approved FY 2021/22 Audit Plan as a contracted information technology (IT) audit. This audit was conducted to evaluate the design, implementation, and effectiveness of the City's wireless network security controls. We contracted with Berry Dunn McNeil & Parker, LLC (BerryDunn), to perform this work, which included a governance controls review and technical assessment of wireless network security controls.

In its review of governance, BerryDunn made recommendations to formalize hardening standards for wireless network components, which will improve the management of security. The technical review did not find any significant issues and made recommendations for enhancing the wireless network's configuration.

We provided a separate confidential report of the results and related recommendations to the IT department. This information is not detailed in the public report due to its sensitive nature.

If you need additional information or have any questions, please contact me at (480) 312-7867.

Sincerely,

Sharron Walker

Sharron E. Walker, CPA, CFE, CLEA
City Auditor

Audit Team:

Paul Christiansen, CIA, CPA, CISA – Sr. Auditor
Lai Cluff, CIA – Sr. Auditor

TABLE OF CONTENTS

AUDIT HIGHLIGHTS

Wireless Network Security

June 10, 2022 Audit No. 2203

WHY WE DID THIS AUDIT

The audit of *Wireless Network Security* was included on the City Council-approved fiscal year (FY) 2021/22 Audit Plan as a contracted audit of a selected information technology (IT) system or area. This audit's objective was to evaluate the design, implementation, and effectiveness of the City's wireless network security controls.

BACKGROUND

The City Auditor's Office contracted with an independent IT audit specialist, Berry Dunn McNeil & Parker, LLC (BerryDunn), to perform this work. The scope of the review included a wireless goverance review, wireless network vulnerability assessment, and risk assessment.

The City's IT department provides wireless access to the Enterprise network at selected City facilities, as well as non-Enterprise (public) wireless internet access at many City facilities. The audit also reviewed potential risks surrounding wireless devices deployed by other City deparments.

City Auditor's Office

City Auditor 480 312-7867
Integrity Line 480 312-8348
www.ScottsdaleAZ.gov

WHAT WE FOUND

IT Governance, Policies and Procedures

The audit identified the following areas where improvements could be made:

- Hardening standards for wireless network components have not been formalized.
- Clarifications and refinement of the definitions and policies for enterprise and "public" wireless networks are needed.

Technical Review

No significant issues were identified in the vulnerability assessments. Security, encryption, and authentication protocols were at the acceptable levels for enterprise class wireless networks, and penetration testing performed was unsuccessful. Detailed findings and recommendations were provided to the IT department and are not detailed in this public report due to the sensitive nature of the information.

WHAT WE RECOMMEND

We recommend the IT department:

- Formalize its wireless network hardening standards.
- Clarify and refine its definitions of enterprise and "public" wireless networks.
- Implement recommended improvements to enhance the technical configuration.

MANAGEMENT RESPONSE

The department agreed with the recommendations and plans to implement changes by the end of calendar year 2023.

BACKGROUND

This audit of *Wireless Network Security* was included in the Council-approved fiscal year 2021/22 Audit Plan as a contracted audit of a selected Information Technology (IT) system or area. The objective of this audit was to evaluate the design, implementation, and effectiveness of the City's wireless network security controls. We contracted with an independent IT audit consultant, Berry Dunn McNeil & Parker, LLC (BerryDunn), to perform this work. The scope of the work included a governance review of policies and procedures relating to the wireless network and a technical assessment of the related security controls.

Wireless Networks

Wireless networking enables devices with wireless capabilities to use computing resources without being physically connected to a network. The devices need to be within a certain distance of the wireless network equipment and exchange data through radio communications. They are usually implemented to provide connectivity to the existing wired network.

Wireless access to the City (enterprise) network is available at some City buildings. This allows users to connect to the City systems and data through their laptops or other wireless devices. In addition, wireless internet access is provided for public and/or staff use at many City facilities – the enterprise network is not connected to this "public" wireless network. These wireless networks are managed by the Information Technology department. As well, several City departments deploy equipment with wireless connectivity that are not be part of the enterprise wireless network and are separately managed by the departments.

While convenient and now widely available, wireless networks also introduce additional security risks to an organization's network. According to the Cybersecurity & Infrastructure Security Agency (CISA), "an attacker could gain access to an organization's network through a wireless access point to conduct malicious activities, including packet sniffing, creating rogue access points, password theft, and man-in-the-middle attacks. These attacks could hinder network connectivity, slow processes, or even crash the organization's system."

According to the National Institute of Standards and Technology's *Guidelines for Securing Wireless Local Area Networks (WLANs),* the security of the wireless network is heavily dependent on the security configuration of each wireless network component. Standardizing, automating, and centralizing the wireless network security configuration allows organizations to consistently implement wireless security throughout the enterprise, detect and correct unauthorized changes, and react quickly to newly identified vulnerabilities or incidents.[1]

[1] National Institute of Standards and Technology (NIST), Special Publication 800-153, *Guidelines for Securing Wireless Local Area Networks (WLANs),* February 2012.

OBJECTIVES, SCOPE, AND METHODOLOGY

An audit of *Wireless Network Security* was included on the City Council-approved fiscal year (FY) 2021/21 Audit Plan as a contracted audit of a selected Information Technology (IT) system or area. The objective of this audit was to evaluate the design, implementation, and effectiveness of the City's wireless network security controls.

We contracted with an independent IT audit consultant, Berry Dunn McNeil & Parker, LLC (BerryDunn), to perform this work. As required by *Government Auditing Standards,* we evaluated the qualifications and independence of these specialists and documented the nature and scope of the specialist's work, including the objectives and scope of work, intended use of the work to support the audit objectives, the specialist's assumptions and methods used, and the specialist's procedures and findings.

To gain an understanding of the City's wireless network infrastructure, the audit team interviewed the Information Technology Director, IT Communications Manager, and Enterprise Communications Specialist that work with the wireless networks. The team also interviewed technology staff from several other departments to learn more about any other separately managed wireless connections. Using the information gathered, BerryDunn worked with the City Auditor's Office to more specifically define the audit scope and methodology:

- IT governance, policies and procedures review – BerryDunn reviewed City and IT policies and procedures and interviewed department management to gain an understanding of IT operations and administrative stance.
- Vulnerability assessment – BerryDunn scanned for identified wireless access points, rogue access points, and vulnerabilities. Auditors selected over a dozen locations across the city for scanning. Data packet captures were gathered at these locations to evaluate security protocols used and perform penetration testing.
- Additionally, BerryDunn assessed risk related to other department managed wireless connections.

BerryDunn applied the following standards in its evaluation of wireless security controls:

- National Institute of Standards and Technology (NIST), Special Publication (SP) 800-153, *Guidelines for Securing Wireless Local Area Networks (WLANs),* February 2012.
- NIST SP800-53 Revision 5, *Security and Privacy Controls for Information Systems and Organizations.*
- Department of Homeland Security: *A Guide to Securing Networks for Wi-Fi,* version 1.0, March 15, 2017.
- Center for Internet Security (CIS) Controls, version 8.

Overall, the security, encryption, and authentication protocols that have been implemented for the enterprise wireless network are at acceptable levels for enterprise class wireless networks. Recommendations were made to improve the City's wireless security posture.

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 work took place from January to April 2022.

FINDINGS AND ANALYSIS

1. IT Governance, Policies and Procedures

BerryDunn reviewed information technology and security policies, procedures and practices related to wireless network architecture, encryption protocols, configuration management, access management, and monitoring. The audit identified the following areas where improvements can be made:

A. Wireless network hardening standards have not been formalized. Documented standards should include minimum acceptable encryption protocols, ports and services, event logging and retention, and patching and vulnerability management. These standards should also define a log retention period and consolidate wireless controller logs with the centralized log server. As with other technology policies and procedures, these standards should be reviewed and updated annually to ensure they remain consistent with the current operating environment.

B. The definitions and policies for enterprise and "public" wireless networks should be clarified and refined. "Public" wireless networks include both password-secured service set identifiers (SSIDs) accessible to employees and open (unsecured) SSIDs accessible by the general public. The definitions should clearly state the business processes, systems that can be accessed, data transmission methods, and acceptable use for each type of wireless network. Additionally, to reduce the potential for City employees to access a less secure wireless network to perform job responsibilities, policies should communicate acceptable uses of each type of wireless network. Further, the SSID naming standard should be evaluated to determine whether it could more clearly reflect the SSID's intended use.

Recommendations:

The IT department should:

A. Formalize the wireless network's hardening standards, including minimum acceptable encryption protocols, ports and services, event logging and retention, and patching and vulnerability management. As well, establish a log retention period and annually review and update policies and procedures.

B. Clarify and refine the definitions and policies for enterprise and "public" wireless networks.

2. Technical Review

The BerryDunn team visited various City facilities to assess the wireless network SSIDs at each location. The team scanned and collected data at each of the selected locations, then evaluated the security configurations and performed penetration testing. Overall, the security, encryption, and authentication protocols implemented were at the acceptable levels for enterprise class wireless networks, and efforts to crack passwords and identify sensitive information were not successful. Based on the configurations observed, BerryDunn recommended configuration enhancements, including not reusing passphrases and reducing the number of SSIDs used.

Detailed findings and recommendations were provided to the IT department and are not detailed in this public report due to the sensitive nature of the information.

Recommendation:

The IT department should implement the technical improvements recommended in the BerryDunn detailed report.

MANAGEMENT ACTION PLAN

1. IT Governance, Policies and Procedures

Recommendations:

A. Formalize the wireless network's hardening standards, including minimum acceptable encryption protocols, ports and services, event logging and retention, and patching and vulnerability management. As well, establish a log retention period and annually review and update policies and procedures.

B. Clarify and refine the definitions and policies for enterprise and "public" wireless networks.

MANAGEMENT RESPONSE: Agree

PROPOSED RESOLUTION:

A. As part of the 22/23 Operating Budget, IT is reclassifying an existing position to Enterprise Wireless Engineer to match similar positions in other valley cities. IT will produce audit-ready documentation of our hardening standards and formalize a log retention period. IT will also work to establish an annual review process for IT policies.

B. IT will refine the definitions, and corresponding policies where needed, to clarify the City enterprise and "public" wireless networks.

RESPONSIBLE PARTY: IT Communications Manager Owen Ellington, Chief Information Security Officer Don Thelander, IT Director Robert Fisher

COMPLETED BY: 6/30/2023

2. Technical Review

Recommendation:

The IT department should implement the technical improvements recommended in the BerryDunn detailed report.

MANAGEMENT RESPONSE: Agree

PROPOSED RESOLUTION: As noted by Berry Dunn and the City Auditor, no critical issues were identified. IT Teams will continue to correct or plan to correct the areas highlighted by Berry Dunn in

their analysis. We will assess additional tools to meet these needs and plan for the procurement of those tools in our budget.

RESPONSIBLE PARTY: IT Communications Manager Owen Ellington, IT Director Robert Fisher

COMPLETED BY: 12/31/2023

City Auditor's Office
7447 E. Indian School Rd., Suite 205
Scottsdale, Arizona 85251

OFFICE (480) 312-7756
INTEGRITY LINE (480) 312-8348

www.ScottsdaleAZ.gov/auditor

CITY OF SCOTTSDALE

The City Auditor's Office conducts audits to promote operational efficiency, effectiveness, accountability and integrity.