TECHNOLOGY & INNOVATION DEPARTMENT
INFRASTRUCTURE SERVICES DIVISION
WIRELESS LAN/WAN SECURITY REVIEW
AUDIT 22-11
AUGUST 22, 2022

City of Tampa
Jane Castor, Mayor

Internal Audit Department
315 E. Kennedy Boulevard
Tampa, Florida 33602
Office (813) 274-7159

August 22, 2022.

Honorable Jane Castor
Mayor, City of Tampa
1 City Hall Plaza
Tampa, Florida

RE: Wireless LAN/WAN Security Review, Audit 22-11

Dear Mayor Castor:

Attached is the Internal Audit Department's report on Wireless LAN/WAN Security Review.

We thank the management and staff of Technology & Innovation Department, Infrastructure Services Division, for their cooperation and assistance during this review.

Sincerely,

/s/ Christine Glover

Christine Glover
Internal Audit Director

cc: John Bennett, Chief of Staff
Dennis Rogero, Chief Financial Officer
Russell Haupert, Director of Technology & Innovation
Eric Hayden, Infrastructure Services Manager
Carl Brody, Assistant City Attorney III

TECHNOLOGY & INNOVATION DEPARTMENT
INFRASTRUCTURE SERVICES DIVISION
WIRELESS LAN/WAN SECURITY REVIEW
AUDIT 22-11
AUGUST 22, 2022

/s/ Stephen Mhere

Senior Auditor

/s/ Christine Glover

Audit Director

TECHNOLOGY & INNOVATION DEPARTMENT
INFRASTRUCTURE SERVICES DIVISION
WIRELESS LAN/WAN SECURITY REVIEW
AUDIT 22-11

BACKGROUND

A local area network (LAN) is a network of interconnected computer technology devices that communicate with each other over short distances such as in a building. When this communication or data exchange occurs using radio transmissions rather than wired connections, the network is a wireless LAN. A wide area network (WAN) is formed by connecting two or more LANs over an extended geographical area.

City of Tampa (COT)'s Technology and Innovation Department (T&I) implements wireless LANs for COT departments that make and fund requests for such networks. Wireless LANs are established to enable Internet access. T&I fulfills these requests through Wi-Fi, a set of network communication protocols that facilitate data exchange without the need for physical wire connections. Although they are convenient, wireless LANs are vulnerable to both unique and familiar information security risks. Some of them are summarized in the table below.

RISK	EXPLANATION OF RISK
Theft of devices	Malicious actors gain physical access to a network device such as an access point. They can compromise the wireless network's information security by tampering with the device, stealing it, gaining access to data on it, and corrupting the data.
Wardriving	A wireless access point's broadcast range can reach as far as the street. Savvy computer users equipped with the right wireless tools (like a powerful antenna) can scan for unsecured networks and identify vulnerabilities. That can be the basis for a malicious attack.
Evil-twin attacks	A rogue wireless access point is set up to broadcast at a stronger signal than a legitimate one. Unsuspecting Wi-Fi users connect to the Internet via the rogue and are at risk of having their personal information stolen, including credit card numbers, passwords to their bank accounts, etc.
Wireless sniffing	Malicious actors use sniffing tools to intercept data in transmission. They might obtain sensitive information such as passwords or credit card numbers.

Two teams in T&I, namely the Unified Communications team and the Security Office, are responsible for wireless LAN/WAN security. These teams have implemented internal controls to protect users, particularly minors, from the dangers of Internet surfing. They also implemented a segregated network architecture, separating COT's wired and wireless networks from each other. By so doing, threats emanating from the wireless LAN do not compromise the confidentiality, integrity, and availability of data in the wired network. In addition, T&I has established general security policies as well as Internet & wireless use policies that provide COT employees with guidance on acceptable use of computer technology, including both the wired networks and wireless LAN/WAN.

STATEMENT OF OBJECTIVES

This audit was conducted in accordance with the Internal Audit Department's FY 2022 Audit Agenda. Audit objectives were to determine if:

1. The system of internal controls for wireless LAN/WAN security is adequate.

2. COT's critical data are sufficiently protected from threats emanating from wireless network vulnerabilities.

3. Internet surfing using COT's wireless networks is safe for minors.

4. COT's wireless access points are located in secure physical environments.

STATEMENT OF SCOPE

The audit period covered Wireless LAN/WAN security activities that occurred in FY 2021 and part of FY 2022. We reviewed these activities to determine whether T&I was fulfilled its stated duties and responsibilities in an effective and efficient manner. Original records were used as evidence and verified through observation and physical examination.

STATEMENT OF METHODOLOGY

We accomplished our audit objectives as follows:

- Evaluated internal controls related to wireless security, including a review of relevant policies, terms and conditions of public Wi-Fi use.

- Reviewed the management of inventory of wireless network equipment.

- Interviewed the infrastructure services manager to discuss his perspective on the risk of fraud and disparity within the wireless network function.

- Toured both Old City Hall (OCH) and Tampa Municipal Office Building (TMOB) to inspect the physical security of wireless equipment locations. This equipment includes routers, security appliances, and wireless access points.

- Surveyed best practice standards for provision of public Wi-Fi by local governments in Florida. We also reviewed legal recommendations for mitigating liability associated with the risk of providing open Wi-Fi to the public.

- Researched performance metrics relevant for wireless network security and provided them to the infrastructure services manager for his consideration.

STATEMENT OF AUDITING STANDARDS

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.

NOTEWORTHY ACCOMPLISHMENTS

T&I's decision to segregate wired from wireless networks is noteworthy. It is a best practice standard recognized by the federal government and is recommended by the National Institute of Standards and Technology.

AUDIT CONCLUSIONS

Based upon the test work performed and the audit findings noted below, we conclude that:

1. The system of internal controls for wireless LAN/WAN security is adequate. However, not all COT Wi-Fi users are getting information about security risks they face on the Internet.

2. COT's critical data are sufficiently protected from threats emanating from wireless network vulnerabilities.

3. Internet surfing using COT's wireless networks is safe for minors.

4. COT's wireless access points are located in secure physical environments.

SPLASH PAGE FOR WI-FI USER AGREEMENT

STATEMENT OF CONDITION: Some COT facilities, including OCH, TMOB, and recreational centers, have Wi-Fi that provides Internet access to City employees and the public. T&I records show that on average, more than 2,600 client devices connect to COT's Wi-Fi on a weekly basis.

Public wireless networks are less secure than wired networks, making information security a major concern when Wi-Fi is used for Internet surfing. In view of this, T&I implemented a splash page that warns the public about this risk. Accessing the Internet via the splash page is an acknowledgement of the risk and of the terms and conditions of service. Some of the terms of service are as follows:

- Users assume, and COT accepts no liability for, risks associated with Wi-Fi use.
- Users will not engage in malicious, offensive, or culturally insensitive activities.
- COT reserves the right to monitor users' Internet activities, and any unauthorized use of resources can lead to criminal liability and claims for damages.

At the time of this audit, some COT facilities, including OCH and TMOB, provided public Wi-Fi without the splash page.

CRITERIA: It is standard practice for local government entities to require users to review and agree to a Wi-Fi user policy containing risk information, liability disclaimer, and terms and conditions of use before they can access the Internet.

CAUSE: The splash page was disabled at OCH, TMOB, and other facilities upon request from COT staff. It was interfering with their work as they had to acknowledge it each time they accessed the Internet. Also, the VPN encryption on COT devices makes them inoperable on public networks that render a splash page. This incompatibility necessitated the deactivation of splash screens at some locations to facilitate the continuation of critical business. T&I is working to find a solution.

EFFECT OF CONDITION: Without the splash page, some Wi-Fi users might not exercise due diligence on the Internet, thereby compromising the confidentiality and/or integrity of their information. This could expose them to the risk of identity theft and COT to legal liability.

RECOMMENDATION: T&I should consider implementing the splash page at all COT facilities. For staff convenience, the page could be programmed to appear on devices once daily. T&I should continue its effort to find a solution that enables the splash page to render on VPN-encrypted devices.

MANAGEMENT RESPONSE: While the Wi-Fi solution in place carries all relevant protections and each employee signs a appropriate use policy when joining the City, we agree with the best practice public offered Wi-Fi service be offered with a standardized information

and warning page and presented in all facilities. T&I is in the process of modernizing the open zones of our Public Wi-Fi service so that we can reactivate the splash screens. We will roll out the solution for zones we have the equipment for this fiscal year and complete the solution with FY 2023 funding where new equipment is required.

TARGET IMPLEMENTATION DATE: March 30, 2023