TECHNOLOGY & INNOVATION DEPARTMENT
REMOTE ACCESS/VPN REVIEW
AUDIT 21-14
FEBRUARY 9, 2022

City of Tampa
Jane Castor, Mayor

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

February 9, 2022

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

RE: Remote Access/VPN Review, Audit 21-14

Dear Mayor Castor:

Attached is the Internal Audit Department's report on Remote Access/VPN Review.

We thank the management and staff of Technology and Innovation Security Office for their cooperation and assistance during this audit.

Sincerely,

/s/ Christine Glover

Christine Glover
Internal Audit Director

cc: John Bennett, Chief of Staff
Dennis Rogero, Chief Financial Officer
Gina Grimes, City Attorney
Russell Haupert, Director of Technology & Innovation
Martin Zinaich, Information Security Officer

TECHNOLOGY & INNOVATION DEPARTMENT
REMOTE ACCESS/VPN REVIEW
AUDIT 21-14
FEBRUARY 9, 2022

/s/ Stephen Mhere

Senior Auditor

/s/ Christine Glover

Audit Director

TECHNOLOGY & INNOVATION DEPARTMENT
REMOTE ACCESS/VPN REVIEW
AUDIT 21-14

BACKGROUND

Remote access is the ability for users to access an organization's non-public computing resources from external or remote locations that may or may not be the organization's own facilities. Remote access can be achieved through dial-up, broadband, wireless, or Virtual Private Network (VPN). For the City of Tampa (City) remote access users may be its own employees, City-affiliated contractors, employees of third-party vendors, or other stakeholders that do business with the City. Some of these users connect to City networks using client devices like desktop computers, laptops, tablets, and smartphones over which the City has no control. As such, the City's information technology infrastructure – both hardware and other resources connected to these devices – are generally exposed to a higher information security risk.

The Technology and Innovation Security Office (TISO) is a division of the City's Technology and Innovation (T&I) Department responsible for the security of the City's information technology assets. As a matter of policy, the City does not authorize remote access or telework to all its employees. It is authorized for personnel that need it for after-hours support, such as T&I employees and personnel from other departments responsible for supporting Public Safety, Water Production, Wastewater, and other critical systems. There were 473 City staff with standing remote access authorization as of May 2021, in addition to the rest of the employees who teleworked due to the pandemic.

STATEMENT OF OBJECTIVES

This audit was conducted in accordance with the Internal Audit Department's FY 2021 Audit Agenda. Our audit objectives were to determine and/or verify that:

1. There are internal controls in place to effectively manage and mitigate information security risks associated with remote access to City networks.

2. City employees, third-party contractors affiliated with the City, as well as employees of third-party vendors receive education, awareness, and training to enable them to recognize and appropriately handle information security threats.

3. TISO uses best practice standards to manage third-party vendor activities on City networks.

4. Reported performance metrics for TISO are accurate, consistent, relevant, and verifiable.

STATEMENT OF SCOPE

The audit period covered remote access activities by TISO in FY 2021. Where relevant, activities in prior years were also reviewed. Tests were performed to determine whether TISO was fulfilling its stated duties and responsibilities in an effective and efficient manner. Among other things, we examined records of remote access activities related to City employees, contractors affiliated with the City, and employees of third-party information technology vendors. We used hard copy evidence to review remote access authorization and electronic evidence of system activities by users.

STATEMENT OF METHODOLOGY

We completed our audit work using the following procedures:

- Evaluation of internal controls for information security relevant to remote access, including policies and procedures as well as established standards.
- Assessment of fraud risk in the information security functional area.
- Review of applications submitted by vendor employees for remote access authorization to City networks and systems.
- Review of TISO's management of third-party user accounts, particularly the process to revoke, deactivate, or remove user accounts from the system.
- Examination of audit logs for selected system users to determine if TISO's management of third-party vendors is consistent with best practice standards.
- Review of the City's Cyber Hygiene Assessment.[1]
- Data reliability assessment for data used or processed through information security applications used by TISO.
- Determination of accuracy, consistency, and relevance of TISO performance metrics.

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

Along with T&I's Infrastructure Services Division, TISO worked long and hard to enable City

[1] A report showing network mapping and vulnerability scanning for Internet-accessible hosts performed by the Cybersecurity and Infrastructure Security Agency (CISA). CISA is an agency of the Department of Homeland Security.

employees to perform their duties through telework during the COVID public health emergency. This was noteworthy because when asked to enable remote access to thousands of employees within a compressed timeline, TISO did so relatively quickly – within a 48-hour period. This was a challenging task to accomplish given the variety of client devices (e.g., regular laptops, MACs, Chrome Books, tablets, etc.) that needed to be set up using dissimilar procedures.

AUDIT CONCLUSIONS

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

1. There are internal controls in place to effectively manage and mitigate information security risks associated with remote access to City networks.

2. City employees and third-party contractors affiliated with the City receive education, awareness, and training to enable them to recognize and appropriately handle information security threats. However, there is not sufficient information to accurately determine or verify if employees of third-party vendors also receive this training.

3. TISO uses best practice standards to manage third-party vendor activities on City networks.

4. Performance metrics for TISO are accurate, consistent, relevant, and verifiable.

INFORMATION SECURITY TRAINING FOR EMPLOYEES OF THIRD PARTIES

STATEMENT OF CONDITION: T&I collaborates with outside entities to provide information technology (IT) services to the City. To enable this collaboration, TISO grants these entities authority to access City networks. In FY 2019 there were 365 individuals from such entities (246 employees from 52 third-party vendors and 119 private contractors affiliated with the City).

Like other local governments, the City operates in an environment fraught with cybersecurity threats. According to MS-ISAC[2], there were 75 ransomware attacks on state, local, and tribal governments between January and June, 2021. Also, a significant number of data breaches (about 51% in 2020 according to one study) are caused by third parties. TISO, has implemented internal control measures to mitigate against information security threats. These include regularly reviewing user access rights as well as system-generated audit logs and revoking, deactivating, or removing users flagged as security risks. TISO also regularly receives and reviews the Cyber Hygiene Assessment which helps identify and secure any weak system configurations and known vulnerabilities in the Internet environment. In addition, TISO has also engaged third parties to assess the cybersecurity rating of its information technology service providers. This gives TISO an independent assessment of the security performance and cyber risk associated with vendor organizations.

Another measure TISO has implemented is the provision of information security awareness, education, and training for both City employees and City-affiliated private contractors. However, our review of policy documents, remote access authorization forms for employees of third-party vendors, and IT contracts did not find evidence that similar training is offered to, or required for, employees of third-party vendors.

CRITERIA: According to industry best practice standards (e.g., Section 7.2.2 of ISO 27002 and the Cybersecurity Maturity Model Certification for federal contractors), users of organizational systems, including employees and relevant contractors of an organization, should receive information security awareness, education, and training.

CAUSE: City contracts do not have provisions or language requiring IT service providers to have information security or cybersecurity training programs for their employees.

EFFECT OF CONDITION: The lack of appropriate language for training of vendor employees in City contracts is a missed opportunity to further enhance cybersecurity. TISO's ability to provide reasonable assurance for data confidentiality, integrity, and availability may be rendered less effective.

[2] MS-ISAC (Multi-State Information Sharing and Analysis Center) is an 11,000-member non-profit organization whose mission is to improve the overall cybersecurity of state, local, tribal, and territorial governments.

RECOMMENDATION: TISO should consider working with Purchasing and Legal to add appropriate language to IT contracts (i.e., future contracts and current ones at the time they are renewed) requiring third-party vendors to implement verifiable information security/cybersecurity awareness, education, and training programs for their employees.

MANAGEMENT RESPONSE: Regarding this finding from a recent remote access review, we would like to address any concerns as they relate to not training employees of third-party support vendors who are not acting as City employees.

- City Cybersecurity Training of 3rd party personnel when acting as City staff does happen as documented during the audit.

- Cybersecurity Training of 3rd party personnel who only provide remote support to their own system is not a common practice in the industry. Such training would require that the City provide training for all employees of a vendor (Microsoft, Oracle… et. al.). We could find no other peer providing such external training to their vendors.

It is important to contextualize such risk when dealing with limited resources and expanding attack surfaces. As noted in the audit, the City of Tampa Security Office has implemented internal control measures to mitigate against information security threats. These include:

- Regularly reviewing user access rights.

- Reviewing system-generated audit logs.

- Revoking, deactivating, or removing users flagged as security risks.

- Regularly receive and review the Cyber Hygiene Assessment which helps identify and secure any weak system configurations.

- Engaged third parties to assess the cybersecurity rating of its information technology service providers. This gives TISO an independent assessment of the security performance and cyber risk associated with vendor organizations.

On this last point, TISO utilizes an independent assessment service to help rate our partners by validating vendor security controls with subjective data. This goes well beyond typical vendor validations of the past. While training is known as a best practice, we could find no relevant peers providing such to 3rd party vendors. However, if this is an agreed upon approach for Legal and Purchasing, the Technology & Innovation Security Office (TISO) stands ready to support any collective effort.

TARGET IMPLEMENTATION DATE: Due to the multi-departmental nature and the potential operational risk of language change in contracts, we plan to complete the project in late October 2022.