AUDIT SERVICES OVERSIGHT COMMITTEE
Monday, February 28th, 2022
Virtual Meeting via Zoom 3:30 P.M.

The Audit Services Oversight Committee met at the above date and time with the following members present: Chair-Nick Long, Vice-Chair-Shanell Frazer, Resident Member Matthew Ruterbories, Mayor Elaine O'Neal, and Council Member Jillian Johnson.

Also present: Wanda S. Page, City Manager; Bo Ferguson, Deputy City Manager; Bertha T. Johnson, Deputy City Manager; Kerry Goode, Director Technology Solutions; DeWayne Kendall, Assistant Director, Technology Solutions; Christina Riordan, Assistant Director, Budget and Management Services Department; Tim Flora, Director, Finance Department/CFO; Karmisha Wallace, Chief of Staff; Dr. Germaine F. Brewington, Director, Audit Services Department, the Audit Services Department Staff; and other guests.

Chair, Nick Long, called the meeting to order at 3:30 p.m.

SUBJECT: APPROVAL OF MINUTES – January 24th, 2022

Motion was made and it was properly seconded to approve the minutes of the January 24th, 2022 Audit Services Oversight Committee meeting.

The motion passed unanimously.

SUBJECT: ADJUSTMENTS TO AGENDA

There were no adjustments to the agenda.

SUBJECT: VPN ACCESS AND DIGITAL TECHNOLGY PERFORMANCE AUDIT PRESENTATION

Dr. Germaine Brewington, Director of the Audit Services Department gave a PowerPoint presentation on the Virtual Private Network (VPN) Access and Digital Technology Performance Audit. Remote work is the practice of employees doing their jobs from a location other than a central office operated by the employer. VPN stands for Virtual Private Network; the City provides remote access by using GlobalProtect VPN. Dr. Brewington stated that this audit was important because as the City allows employees to have a flexible work schedule to include remote work, it is essential that the City has internal controls and safeguards in place to mitigate security risk.

There are several policies in place to provide guidance for remote work: ITP-1 Use of Information Technology Resources; ITP-4 Information Technology Security Policy; and Technology Solutions GlobalProtection VPN process.

Dr. Brewington discussed the objectives of the audit: 1.) to review controls over VPN access, including monitoring and maintenance practices; and 2.) to review practices and procedures around issuing MIFI/Hotspots devices.

Overall, Technology Solutions Department (TS) has controls in place to ensure only authorized employees and vendors are granted access to the City's systems; an employee's access is terminated when they leave the City; and, monitoring of VPN access is being performed. Periodic reviews are not currently being documented-but should be; steps need to be taken to ensure sensitive data is not stored on devices in this remote work environment; and City leadership in conjunction with Human Resources (HR) should collect and analyze data to ensure digital requests are being equitably evaluated and decisions are being equitably applied.

Finding 1: Periodic vendor review is required by the Department's Standard Operating Procedure (SOP); but, documentation did not exist to support the reviews.
The GlobalProtect VPN process SOP requires quarterly monitoring of vendor access. Information on vendor access such as vendor start date, and the duration of that access is not retained by the Technology Solutions Department. This information would help facilitate those quarterly reviews.

Finding 2: Procedures do not address the handling and protecting of sensitive data stored on remote work devices.
The NIST SP 800-46 Rev. 2 guidelines provide a framework for mitigating risks for data security. Providing awareness to employees regarding protocols for storing sensitive information can mitigate risks to data security.

Finding 3: Data is not available to determine if the current process of assigning MiFi devices results in equitable distribution of those devices.
At present, the Flexible Work Request Form provides an opportunity for employees to identify new or additional equipment/technology needed to successfully complete their work from a remote location. Currently, data is not being collected or analyzed for these requests to determine if the distribution of digital technology is equitable or conforms to the City's equity initiative.

Recommendation 1 (Management Concurred)
The Technology Solutions Department staff should ensure that periodic vendor access reviews are performed in accordance with the GlobalProtect VPN Process Standard Operating Procedure. In addition, supporting documentation of the review should be retained and information such as vendor access start date and duration of access approved should be retained in the Boss ticketing system.

Value Added*: Risk Reduction; Compliance*

Recommendation 2 (Management Concurred)
The Technology Solutions Department staff should implement practices to ensure sensitive information, such as certain types of Personal Identifiable Information – PII (e.g., personnel records, medical records, financial records), is protected and not

stored on devices. The Technology Solutions Department should also incorporate the handling of sensitive information as part of its training program.

Value Added: *Risk Reduction*

Recommendation 3 (Management Concurred)
City leadership should work in conjunction with Human Resources staff to collect data on technology requests that are part of the Flexible Work Request Form. This data should be analyzed to determine if digital requests are being equitably evaluated and decisions are being equitably applied.

Value Added: *Risk Reduction; Compliance*

Questions/Comments:

Questions by ASOC members:

Chair Nick Long asked if there was any data on people who were denied MiFi's due to resources in the department?

Dr. Brewington said no. Currently the Human Resources (HR) staff do not know since there has been no data collected to track this. There is an approval and denial section on the Flexible Work Requests form but that information has not been captured. This lack of collected data is one of the reasons Audit staff suggest this data be collected and analyzed to facilitate data driven decisions around equity in this space.

Resident Member Ruterbories asked in regards to Finding 1, if the City has a "bring your own device" policy or any sort of policy covering the use of employee owned devices to access the City's system via the VPN or email; or is it strictly City owned assets that can access the network?

Dr. Brewington stated each person that is working remotely from home has been issued a City owned device. Each employee has GlobalProtect on the City issued device, which is how we access City systems. Dr. Brewington welcomed Technology Solutions (TS) Director Kerry Goode to comment.

Kerry Goode, Technology Solutions Director stated at the present employees must have a City owned device to access City systems. However, as we move forward with implementing Mobil Device Management we may consider "bring your own device" as part of the environment. At the moment since we do not have Mobil Device Management, employees need to have City issued devices to access the City's systems. We are anticipating moving forward with new technologies and plan on introducing a policy, if City Manager Page signs it, that will allow City employees to "bring your own device" and access virtual PC's as part of that process.

Resident Member Ruterbories had a question on Finding 2 – addressing Personal Identifiable Information on a user device. What I'm understanding from the discussion, is what we really are referring to are controls and procedures around data stored physically on an employee device. But what we are really getting at is that employees need to understand that data should not be stored locally. Is that the gist of the recommendation?

Dr. Brewington confirmed yes, that's exactly right. She discussed a prior incident that occurred months ago. Some City sensitive information was compromised; but it wasn't compromised because of something that happened on the City's end. The receiver of that information was where the compromise occurred. That incident brought to light the City's vulnerability with regard to sensitive information saved on a City employee's device; information the employee was not really aware was there. The information was on her device because of the way the information had to be retrieved out of MUNIS (City system), saved and then submitted to the customer. The compromise of City information, while not the fault of any City employee, brought to light, that we need to bring more attention and awareness to City employees about sensitive information being stored on their devices.

Kerry Goode, Director of Technology Solutions, added that the information was an unstructured document. Unstructured means the data was pulled from a structured table into a spreadsheet document and it was uploaded to the State's site but was not removed from the local device. Undoubtedly, the incident could have introduced risks for the organization if the compromise had originated from the City.

DeWayne Kendall, Assistant Director of Technology Solutions added that our structured data tables are in one of our most secured locations. Where our structured data resides in the ERP system, which houses all of the HR and Finance modules, those modules have been cited by outside auditors as one of our most secured locations. Those tables are very difficult to penetrate based on the security posture of the City.

Resident Member Ruterbories asked a final question related to Finding 3. I hear the need for the equitable distribution of the MiFi devices, but I'm wondering if throughout the last two years the City has revisited any of its benefits offerings or has plans to revisit any of the benefits offerings to support employees working from home. I'm talking about things like future state -bring your own computer or phone for teleconferencing, or opportunity to reimburse employees for upgraded internet coverage, that sort of thing. I am wondering if the City has discussed any plans to promote this equitable distribution of resources?

City Manager Wanda Page stated –often there are conversations of different kinds on equity and innovative ideas as an organization. To answer you specifically, in the sense of a deep equity discussion, we have not advanced any proposals beyond the proposals we currently have around the flexible work policy. We do have some programs that enable every City employee to access a phone or smart phone in order to be able to access City emails. We have been working on that for a really long time; and some of this came about due to the pandemic. At least every person has access to a smartphone. For folks that want to use their own devices as it's related to mobile devices, like a phone, we have an option for having a monthly allowance for phones (City business) and we do have policies around that as well. We have started to look into more

equitable pay and benefits and we started this last fiscal year, when we considered our bonuses—that were based upon levels of annual salary in the organization—through an equity lens. So employees at lower ends of the salary range received a higher bonus than employees at higher ends. We have begun to view everything we do through an equity lens. That is one of the reasons, I believe you actually see this language around Recommendation 4, that the auditor has presented, due to us looking for ways we can apply this equity lens in pretty much everything we do and in every department. You will begin to see more conversation around equity coming forward in the future. So hopefully this is the kind of response you will see, as well as some additional conversations around what we are doing in the organization as we move into intentionally thinking of equity for our employees.

Resident Member Ruterbories thanked Madam Manager Page for her response.

SUBJECT: DISCUSSION OF THE PROCESS FOR THE DEVELOPMENT OF THE ANNUAL AUDIT PLAN

Dr. Brewington moved on to discussing the Annual Audit Plan process. The Audit staff conducts a risk based assessment every year to develop an Annual Audit Plan, the City's Annual Audit Plan. Dr. Brewington explained the process begins with the Audit staff requesting information and or ideas from ASOC (Audit Services Oversight Committee) members and department directors regarding audits to perform. The Annual Audit Plan Input Form – Fiscal Year 23 (FY) was emailed to the ASOC members so the members can, if they have an idea or a process they would like the Audit staff to examine more closely they can write the idea on the form and email it to the staff. Dr. Brewington stated that the Audit staff also look across the country at Local Government Internal Audit shops, especially our sister Cities, to see what the other Internal Audit shops are looking at, what issues are trending. Audit staff conducted a Jamboard session (that's a tool in Google that allows you to interactively have a discussion and solicit ideas) at the last directors meeting and Audit staff received over 30 ideas for audit topics for this next Facial year 2023 Annual Audit Plan. FY 2023 is the second year using Jamboard to gather these ideas. Dr. Brewington stated that her colleagues are the experts in their various businesses. Having these experts help the Audit staff shape the Annual Audit Plan, has been invaluable because that means Audit staff are spending their limited resources and capacity in the right areas.

Next, Audit staff will compile the input from everyone and around mid-March to the end of March Audit staff will run all of these different processes through their risk model. Staff will compare that list to the City wide enterprise risk model to ensure they are looking at processes that line up with the six risks categories the City leadership deems critical at the time; including public safety, talent and retention, community growth impact, systems, communication and one other.

The final step includes the Audit staff, prior to the April meeting, sending out the results of the compilation and analysis (the entire list along with the staff's proposal of the top ten to twelve audits to be performed in FY 2023 in priority order based on risk rankings). Distribution of the list by the second week in April, will give you time to review and formulate some questions to

have a robust discussion at the April meeting. During that meeting you are welcome remove any item or re-rank the items on the list. We have already received input from directors, so we will continue this process and in April we can have a robust discussion on the items that end up on that list.

OTHER BUSINESS

There was no other business to discuss.

Dr. Brewington stated a reminder for Chair Long. In the June meeting you, the committee, will have to select new officers for FY 2023 beginning in July. Usually that nominating committee gets together 30-45 minutes prior to that meeting. The committee needs to select a nominating committee for that process.

Council Member Johnson stated she will be out of town for the March meeting and will ask Council Member Freeman to attend as the alternative.

Next meeting is scheduled for March 28th, 2022. The meeting will begin at 3:30 p.m. and it will be virtual.

Chair Nick Long adjourned the meeting at 4:13pm

Respectfully submitted,

Francisca Fabian