COUNCIL REPORT – OFFICE OF THE CITY AUDITOR

CYBER SECURITY PROGRAM AUDIT

RECOMMENDATION

1. That the May 8, 2023, Office of the City Auditor report OCA01877, be received for information.
2. That Attachment 1 of the May 8, 2023, Office of the City Auditor report OCA01877, remain private pursuant to sections 20(1)(m) (disclosure harmful to law enforcement), 24(1)(a) (advice from officials) and 25(1)(c) (disclosure harmful to economic and other interests of a public body) of the *Freedom of Information and Protection of Privacy Act*.

Report Purpose

Information only.

Executive Summary

The Cyber Security Program Audit report is attached. Due to the nature of the audit and its recommendations, the report is recommended to be kept private pursuant to sections 20(1)(m) (disclosure harmful to law enforcement), 24(1)(a) (advice from officials) and 25(1)(c) (disclosure harmful to economic and other interests of a public body) of the Freedom of Information and Protection of Privacy Act. The report contains details that could be used to compromise critical City systems, bringing harm to the City's economic interests or life safety systems. Audit recommendations should also be kept private.

REPORT

Cyber security is the practice of protecting the City's digital assets[1] from attacks. The Corporate Information Security Office (CISO) oversees cyber security at the City. They maintain the Cyber Security Administrative Directive and the associated standards, specifications, plans, and requirements. The CISO is situated within the Open City & Technology (OCT) Branch. The City

[1] Digital assets include information technology infrastructure, telecommunications, networks, laptop computers and tablets, application software, and data.

contracts with two third-parties who provide cyber security monitoring, detection and analysis services.

The National Institute of Standards and Technology (NIST) develops best practice guidelines for a cyber security program. The NIST cyber security framework consists of five domains:

- **Identify** - Understand and manage cyber security risks
- **Protect** - Develop safeguards over cyberspace and digital assets
- **Detect** - Develop practices to identify cyber security events
- **Respond** - Develop practices to respond to cyber security events
- **Recover** - Develop plans to restore services that were impaired due to a cyber security event

The objective of this audit was to determine whether the CISO is managing its cyber security program to protect the City from security threats. Edmonton Transit Service and Waste Services Branch manage specialized operational technologies that are not within the purview of the CISO office[2]. Cyber security of these technologies was outside the scope of this audit.

We found that 14 of the 23 control categories met most or all of the expectations, 6 categories met some of the expectations, and 3 categories met few. In Appendix A, we prepared a summary of the effectiveness of the controls by NIST domain and category.

The CISO understands and manages cyber security risks through a detailed cyber security risk register that is updated quarterly. Many data protections are in place, including vulnerability management, regular backups, encryption of backups, maintaining baseline configurations, and capacity monitoring. OCT and the CISO have effective practices in place for detecting, responding to, and recovering from cyber security incidents. They identify abnormal activities through continuous monitoring of devices, network perimeter, email and Google Cloud Services, and understand the potential impact of these activities. The CISO has developed a Cyber Security Incident Response Plan, and regularly tests and updates it.

However, we identified controls that could be improved and made nine recommendations around data, user access, networks, change management, security assessment, vendor management and staff training. Specific information related to these control improvements and recommendations to address them are included in Attachment 1.

POLICY

Bylaw 16097, Audit Committee Bylaw, Section 14(d) states that, “Committee will review all reports from the City Auditor dealing with completed audit projects.”

ATTACHMENT

1. Cyber Security Program Audit Report (Private)

[2] Operational technology (OT) is hardware and software that detects or causes a change, through the direct monitoring and/or control of industrial equipment, assets, processes and events. The Branch Managers of these areas are accountable for those digital assets, including cyber security per *A1473 - Cyber Security Administrative Directive*.

CYBER SECURITY PROGRAM AUDIT

APPENDIX A - SUMMARY ASSESSMENT

The NIST cyber security framework is organized into five domains (Identify, Protect, Detect, Respond, Recover). Each domain consists of categories, which are further divided into subcategories. Our assessment of each category is in the table below. The colours correspond to subcategory controls expectations:

Green - no control deficiencies

Yellow - some control deficiencies

Red - many control deficiencies

Domain	Category
Identify	Asset Management
	Business Environment
	Governance
	Risk Assessment
	Risk Management Strategy
	Supply Chain Risk Management
Protect	Identity Management, Authentication and Access Control
	Awareness and Training
	Data Security
	Information Protection Processes and Procedures
	Maintenance
	Protective Technology
Detect	Anomalies and Events
	Security Continuous Monitoring
	Detection Processes
Respond	Response Planning
	Communications
	Analysis
	Mitigation
	Improvements
Recover	Recovery Planning
	Improvements
	Communications