TORONTO

REPORT FOR ACTION

2025 Chief Information Security Officer's Report on Agencies and Corporations

Date: October 20, 2025
To: Executive Committee
From: Chief Information Security Officer
Wards: All

SUMMARY

In May 2024, City Council directed the Chief Information Security Officer, through item 2024.EX14.3, to extend its mandate to include oversight of City agencies and corporations and to report annually in October to the Executive Committee on their responses and compliance rates.

Overall, nearly all City agencies and corporations have executed agreements with the Office of the Chief Information Security Officer and a core suite of cyber security services, including continuous cyber monitoring, has been deployed. Additionally, the Chief Information Security Officer has increased strategic collaboration with leadership teams from each agency and corporation through the Executive Cyber Risk Management Group, further enhancing policy development, program enhancement, and threat response across the cyber landscape. These combined efforts have led to a 37% improvement in overall cyber resilience since last reported to City Council in November 2024.

This report provides information about the progress that the Chief Information Security Officer has made in operationalizing and sustaining the directions of City Council in 2024.EX14.3.

RECOMMENDATIONS

The Chief Information Security Officer recommends that:

1. City Council receive this report for information

FINANCIAL IMPACT

The Chief Information Security Officer will continue to monitor financial impacts associated with this extended mandate through future budget processes.

The Chief Financial Officer and Treasurer has reviewed this report and agrees with the financial implications as identified in the Financial Impact section.

DECISION HISTORY

At its meeting on November 13 and 14, 2024, City Council adopted item 2024.EX18.6 - 2024 Chief Information Security Officer's Report on Agencies and Corporations, providing the first annual update on the implementation of the Chief Information Security Officer's expanded mandate. https://secure.toronto.ca/council/agenda-item.do?item=2024.EX18.6

At its meeting on May 22 and 23, 2024, City Council adopted item 2024.EX14.3 - Extending the mandate of the City's Chief Information Security Officer, which expanded the mandate of the Chief Information Security Officer to include working with the City's agencies and corporations to improve overall cyber posture, and report annually to the Executive Committee. https://secure.toronto.ca/council/agenda-item.do?item=2024.EX14.3

COMMENTS

Council Direction

On May 22 and 23, 2024, City Council directed the Chief Information Security Officer to collaborate with and assist the City's agencies and corporations to do the following:

- Provide the necessary information, access, and visibility into their cyber security programs to facilitate the cyber security risk management partnership with the Chief Information Security Officer;
- Operationalize the Chief Information Security Officer's recommendations to mitigate cyber risks identified in the cyber security risk management partnership;
- Engage in consultation with the Chief Information Security Officer on all initiatives that could potentially affect cyber security, including but not limited to, rates of compliance, remediation plans and strategies aimed at reducing risks and promoting compliance; and,
- Align their organizational cyber security frameworks with the City's overarching cyber security objectives, the City's Digital Infrastructure Strategic Framework, and established international cyber security standards.

The foundation for the City's cyber relationship with agencies and corporations are cyber policies and standards, published by the Chief Information Security Officer which provide a consistent framework for protecting sensitive information, mitigating cyber risks, and maintaining regulatory compliance. The policies and standards are informed

by a comprehensive set of internationally recognized standards, frameworks, and regulatory requirements, including, but not limited to, International Organization for Standardization (ISO)/ International Electrotechnical Commission (IEC) standards, National Institute of Standards and Technology (NIST) Special Publications, the NIST Cyber Security Framework (CSF), Statement on Standards for Attestation Engagements (SSAE) standards, International Society of Automation (ISA)/IEC industrial cyber security guidelines, and Payment Card Industry Data Security Standard (PCI DSS).

The City's Confirmation Program for agencies and corporations was incorporated into the Chief Information Security Officer's extended mandate.

Implementation of Extended Cyber Security Mandate for Agencies and Corporations

Following City Council's direction in May 2024, the Chief Information Security Officer adopted a strategic and phased approach to operationalize and sustain the extended cyber security mandate across City agencies and corporations.

To support this initiative, an onboarding package was distributed to all agencies and corporations. This package outlined the cyber security services available and included legal documentation establishing the collaborative framework for service delivery under 2024.EX14.3. Of the 40 agencies and corporations identified in 2024.EX14.3, 98% (39) have executed agreements to receive cyber security services and support through the extended mandate. Additionally, discussions between the Chief Information Security Officer and the remaining organization identified in 2024.EX14.3 are ongoing.

The Chief Information Security Officer met with leadership teams from each organization to review the mandate, present service offerings, understand specific needs, and address concerns. Additionally, the Chief Information Security Officer engaged with boards of agencies and corporations that expressed interest, particularly among the largest organizations, due to the complexity of their IT environments.

Cyber security experts from the Office of the Chief Information Security Officer conducted multiple engagements with technical staff across all participating agencies and corporations. These sessions focused on assessing cyber security needs, reviewing existing solutions, identifying services to be leveraged, and prioritizing implementation. These efforts have enabled the deployment and sustainability of tailored cyber security solutions.

In addition to the technical engagements with the agencies and corporations, the Executive Cyber Risk Management Group (ECRMG), led by the Chief Information Security Officer or their delegate, convenes twice a year and includes administrative heads and technical leaders of agencies and corporations. This forum provides strategic guidance on policy development, program enhancement, threat landscape updates, and service roadmaps. The ECRMG also fosters collaboration and information sharing among participating organizations.

Current State

Several cyber security services have been fully deployed and are operational across agencies and corporations, with 24/7/365 monitoring in place. The initial core services identified at the outset of the extended mandate have been successfully implemented. Additional deployments are underway, and new services are introduced annually to meet evolving needs.

The extended mandate has been well received. The cyber posture across City agencies and corporations has significantly improved, with an overall increase of 37% in evaluated resilience since last reported in November 2024.

CONTACT

Andree Noel
Deputy Chief Information Security Officer
(416) 392-8699
Andree.Noel@toronto.ca

SIGNATURE

Maneesh Agnihotri
Chief Information Security Officer