Job Title	Senior Specialist Urban Technology Protection (Emerging Technology)
Division	Office of the Chief Information Security Officer
Reports To	Manager Threat Intelligence & Fulfillment
Salary Range	$110,947.20 to $130,353.60
Work Location	55 John Street, Toronto
Job Type	Permanent Full Time
Shift Information	Monday to Friday, 40 hours work week
Posting Closing Date	May 3, 2021

JOB SUMMARY:

To provide subject matter expertise, strategic advice, senior level guidance and operational support for the development, delivery, sustainment and protection of critical infrastructure and emerging technologies that will assist in detecting, monitoring and predicting cyber risk.

To engage with teams across the organization to build alignment on key projects and initiatives and develop execution roadmaps.

To support the execution of the Chief Information Security Officer's (CISO) mandate, cyber vision and strategy, providing technical and business advice, support and services to all City divisions, agencies and corporations.

MAJOR RESPONSIBILITIES:

- Develops and implements detailed plans and recommends cyber security policies/procedures regarding program specific requirements.
- Supervises, motivates and trains assigned project staff and contract resources, ensuring effective teamwork, high standards of work quality and organizational performance, continuous learning and encourages innovation in others.
- Supervises the day to day operation of all assigned project staff and contract resources, including the scheduling, assigning and reviewing of work. Coordinates vacation and overtime requests. Monitors and assists in evaluating staff performance, hears grievances and recommends disciplinary action when necessary.
- Provides direction, leadership, guidance and advice to project teams, assigned project staff and contract resources. Oversees and reviews their work.
- Provides leadership to influence employee engagement to the organization, to the team, and to their role.
- Conducts research into assigned area ensuring that such research takes into account developments within the field, corporate policies and practices, legislation and initiatives by other levels of government.
- Provides input into assigned project budgets, ensuring that expenditures are controlled and maintained within approved budget limitations.
- Provides subject matter expertise and strategic advice on cyber security issues affecting the organization, identifying potential exposures, and conducting reviews to ensure that

undesirable effects are detected, mitigated and/or corrected, and providing pragmatic advice to clients to ensure that cyber risks are managed appropriately.

- Serves as the internal/external point of contact and subject matter expert in critical infrastructure and emerging technology protection, sustainment, development and delivery.
- Anticipates, analyzes and identifies organizational impacts of emerging requirements; recommends and coordinates innovative solutions using conflict resolution and negotiation skills to successfully manage sensitive and controversial matters.
- Participates in the development of transformation strategies focused on security, integrating and managing new or existing technology systems to deliver continuous operational improvements and detect, respond, and remediate threats.
- Resolves cyber risk issues. Escalates significant cyber risk matters to senior management when required.
- Deals with confidential information affecting the organization and its resources. Prepares and presents reports to management supporting recommendations on changes/improvements in business processes, training and services standards that impact appropriate staffing levels and resource allocation. Makes recommendations based on investigation results which could lead to the discipline or dismissal of staff.
- Participates in the development, implementation, administration, monitoring and maintenance of security tools collecting confidential information on infrastructure and application weaknesses Maintains up to date knowledge of City's confidential cyber infrastructure.
- Works with senior management within the division to address active internal/external cyber threats to the City. Attends senior management meetings, makes recommendations to mitigate the threats, and takes appropriate urgent action as needed.
- Provides a confidential assessment of organizational issues and makes recommendations for next steps, including policy, procedural and structural change.
- Leads the delivery and sustainment of adequately protected critical infrastructure and emerging technologies. Works with clients to develop solutions for critical infrastructure and emerging technologies that will assist to detect, monitor, and predict risk.
- Determines cyber security requirements of business strategies in order to provide appropriate advice, guidance, and technical solutions.
- Designs the proper sets of Operational Technologies (OT) and Internet of Things (IoT) security architecture controls to ensure authenticity, non-repudiation, and least privilege commensurate with risk requirements.
- Performs cyber review of OT and IoT technologies in targeted processes across all areas of the organization. Designs, develops, tests, and implements security controls in Emerging Technology (Emerging Technologies (e.g. Election Technologies, Autonomous Vehicles, 5G, Blockchain, Artificial Intelligence, Quantum Sensing)) projects.
- Facilitates key decisions involving IoT, OT and Emerging Technology architecture and systems.
- Collaborates with teams across all areas of the organization to understand the business direction and consequent impact on the security posture of the existing IoT, OT and Emerging technologies.
- Identifies architectural and other security risks associated with the IoT and OT projects, and compensating controls where necessary.
- Leads the development and implementation of enterprise information security requirements across the OT environment.
- Develops and maintains an understanding of the current state of the IoT and OT information

security environment, including gaps and risks, and identifies and leads opportunities for improvement.

- Develops roadmaps for information security technology solutions in IoT and OT and oversees any issues through to resolution.
- Works with the business integration leads to identify technology specific requirements and assess new technologies for applicability.
- Leads the technical integration between information technology and IoT and OT requirements, including supporting the identification of data point connections for metrics and reporting.
- Performs architecture security reviews and develops scenarios that can be tested in either production or laboratory environments for smart city.
- Reviews system-related materials including specifications, diagrams, requirements and tests plans to ensure security-related standards are followed.
- Reviews assessment results with system owners and senior level stakeholders and provides recommendations based off of gathered metrics.
- Creates comprehensive cyber architecture assessment reports including remediation strategies for urban infrastructure technologies.
- Works collaboratively with teams to implement and support existing and future Smart City security solutions.
- Defines common toolsets at the process controls network level to enable the City's information security metric and KPI stewardship at the strategic, tactical, and operational levels.
- Develops, reviews, and ensures approvals of security strategies within industry-accepted frameworks.
- Provides leadership in the evaluation, selection and recommendation of technical solutions and professional services. Identifies and evaluates emerging security technologies.
- Takes a proactive approach to identify gaps and opportunities for improvement to mitigate risk.
- Organizes and works with multidisciplinary business and technical teams from across the organization to formulate and execute project plans and tasks according to established project management principles and methodologies.
- Provides oversight and monitors cyber risk activities performed by project teams. Reviews and supports the implementation of processes and controls by various teams as outlined in the information risk policy and related operating directives, standards and procedures.
- Provides project coordination and management support, and ensures comprehensive and effective information communication across various functional and project teams.
- Communicates effectively to stakeholders, clients, project managers, and team members regarding any business and technical decisions and actions that may impact solution delivery, staff performance, business processes, management workflow and technical support of public services.
- Provides support in the design, implementation, maintenance, and enforcement of policies, procedures, and controls.
- Plans, prioritizes and coordinates internal and/or external assigned project resources to meet project objectives.
- Prepares and/or supervises the preparation of various formal contractual documents such as Request For Information/ Proposal/Quotation, Statement of Work, Memorandum of Understanding and Service Level Agreements.
- Maintains accurate reporting of key risk metrics and associated measurements in alignment

with the cyber risk appetite.
- Prepares regular cyber risk management reports, briefing notes, and presentations as required, leveraging cyber risk subject matter expertise.
- Builds and maintains strong relationships with internal and external stakeholders. Establishes relationships with strategic partners, collaborating on the advancement of cyber programs.
- Participates in meetings with executive leadership and strategic partners to review City's cyber security posture.
- Maintains an up-to-date and in-depth knowledge of cyber security, emerging threats, trends, and associated techniques and technologies as well as key business drivers and opportunities.

QUALIFICATIONS/CERTIFICATIONS:

- Post-secondary degree in Engineering or Technology or a related discipline
- Over 6 years' experience in Information Security.
- In-depth knowledge of industry standards and best practices, especially related to industrial environments in the cyber security space.
- Extensive experience with Industrial Control Systems, PLCs, and SCADA Systems
- Extensive experience with Emerging Technologies (e.g. Election Technologies, Autonomous Vehicles, 5G, Blockchain, Artificial Intelligence, Quantum Sensing)
- Technical expertise in IT/OT integration and convergence.
- Familiar with process safety risk, process hazard analysis, control system analysis, and layer of protection analysis.
- Expertise in security protection solutions including firewall, intrusion detection and protection systems, web application firewalls, anti-virus, and security monitoring solutions.
- Preferred Certifications (any in the list): CISSP, CTIA IoT, CCSP, CISM

SKILLS:

- Ability to work in transformative programs.
- Ability to lead efficient communication between all project stakeholders, including internal teams and clients
- Ability to achieve business objectives through influencing and effectively working with key stakeholders.
- Excellent written & verbal communication skills (comfortable & confident communicating at all levels including business partners, leadership and vendors.
- Excellent problem-solving skills with capability to identify solutions to unusual and complex problems.
- Keen attention to detail and strong organizational skills.
- Highly organized, proactive, self-motivated team player who takes initiative and is able to work independently.
- Ability to work in a fast-paced environment managing multiple priorities with proven time management skills.
- Strong analytical skills and ability to prioritise and multitask.
- Ability to prioritize and effectively manage competing priorities and projects.
- Ability to manage multiple initiatives while adhering to strict deadlines.
- Able to work extremely well under pressure while maintaining a high level of professionalism
- Self-motivated person with desire to go above and beyond tasks
- Transferable skills, like communication and decision-making, are equally important.

- Being able to think on your feet and show good judgment are especially valuable in this field. “Security pros should always be ready to react to cyber-related incidents quickly.

ADDITIONAL COMMENTS/INFORMATION:

A normal work week is 40 hours, however, unforeseen situation may require extended hours of work with little or no prior notice. In case of a cyber incident or breach, rotation shift, continuous extended hours may be required with little or no prior notice.

*Subject to a police check, background check, psychological assessment and/or any other checks on a regular basis as the Office of the CISO handles highly sensitive and confidential information.

EQUITY, DIVERSITY AND INCLUSION

The City is an equal opportunity employer, dedicated to creating a workplace culture of inclusiveness that reflects the diverse residents that we serve. Learn more about the City’s commitment to employment equity.

ACCOMODATION

The City of Toronto is committed to creating an accessible and inclusive organization. We are committed to providing barrier-free and accessible employment practices in compliance with the Accessibility for Ontarians with Disabilities Act (AODA). Should you require Code-protected accommodation through any stage of the recruitment process, please make them known when contacted and we will work with you to meet your needs. Disability-related accommodation during the application process is available upon request. Learn more about the City’s Hiring Policies and Accommodation Process.