CANADIAN INSIDER THREAT DATASET

White Paper

Canadian Insider Threat Dataset Taskforce

Ottawa, Ontario, Canada

CanadianInsiderRiskManagementCOE@carleton.ca

CANADIAN INSIDER RISK MANAGEMENT CENTRE OF EXCELLENCE

Canadian Insider Threat Dataset (CITD) White Paper

The Threat Environment

Over the past decade, the Canadian insider threat environment has seen a notable shift, mirroring international Five Eyes (FVEY) nation-states' concerns about data breaches, espionage, and other malicious or negligent insider threat activities. Threats that may emanate from those within an organization with privileged levels of access to critical assets and personnel (employees, contractors, or associates) may inflict harm, divulge sensitive information, or involve fraud.

Given Canada's advanced economy, technological advancements, and key role among its Western allies, it is an enticing target for adversaries. The country's federal government institutions, critical infrastructure private owners and operators, and research-intensive academic bodies possess sensitive data that, if compromised, could have cascading consequences on national security, economic stability, and Canada's global standing.

In is, therefore, imperative for our institutions to foster a culture of collaboration, and to share intelligence and best practices on insider threats. A holistic approach, integrating insights from the private, public, and academic sectors, ensures a comprehensive understanding of the evolving threat landscape and a united strategy to mitigate the associated risks.

EXECUTIVE SUMMARY – CITD

- The Canadian security community, across private, public, and academic sectors needs to be sharing information related to insider threat incidents, to foster situational awareness of the evolving threat environment as well as build on best practices.
- The implementation of a CITD based on the necessary security safeguards and third-party assurance controls will **foster a community-of-trust** among industry participants and for Canadian insider risk management practitioners to consult with one another on a routine basis.
- Information sharing of insider threat compromises will be difficult in the beginning as there is presently a significant negative industry stigma associated to the revelation of compromise that impacts organizations' reputations. Ensuring participants' full anonymity will be critical.
- Standardized reporting will enable a realistic and broad understanding of the frequency and scope of insider threats in Canada and across multiple industries.
- The voluntary sharing of information to support trend reporting and industry advocacy is a choice that empowers victim organizations; otherwise, industry partners and the Canadian public at large, are only learning about compromises based on media reporting.
- The best way forward for the CITD is to require the minimal amount of incident details to be shared at the beginning for all participants to gain valuable insights and continue to support the long-term objectives of the initiative and provide more information in the future.
- Information standards differ across government and industry. Having an agreed upon minimal standard would be a positive step towards gathering valued insight.
    - Example: the IT architecture and control standards applied to the security of insider threat incident data being proposed for the CITD, should ensure data encryption while at-rest and in-transit, as well as Canadian residency.

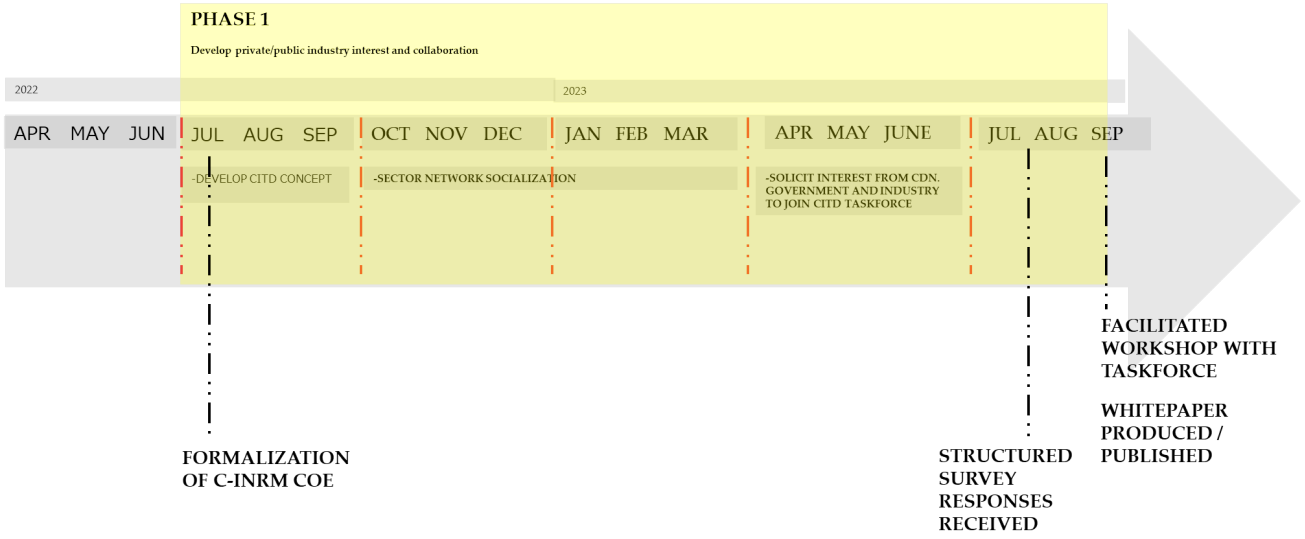
BACKGROUND – CANADIAN INSIDER THREAT DATASET

Data analytics plays a pivotal role in modern-day insider risk management, enabling organizations to proactively detect patterns and anomalies that signify potential threats, and potentially enabling proactive intervention and the enhanced protection of organizational assets. Insider threat and risk modelling is based on attributes found in representative past use cases of known attacks, and statistical correlation is stronger when there is greater variation found in attributes from past use cases. However, organizations are generally only using their own incident data, found within their Security Information and Event Monitoring (SIEM) database repositories, for risk modelling. Accessing information about the attributes associated to other insider threat compromises, sourced from other Canadian organizations within their respective critical infrastructure sectors, is not available. Further, in academia, rigorous research on insider threats and risk mitigation based on real case studies with moderate to large sample sizes, does not generally exist.

Canada lacks a national dataset of incident reporting for industry risk mitigation and academic research purposes. There is no centralized, secure portal, for information sharing and aggregation for analysis, or a standardized insider threat incident reporting taxonomy.

CITD Phase 1

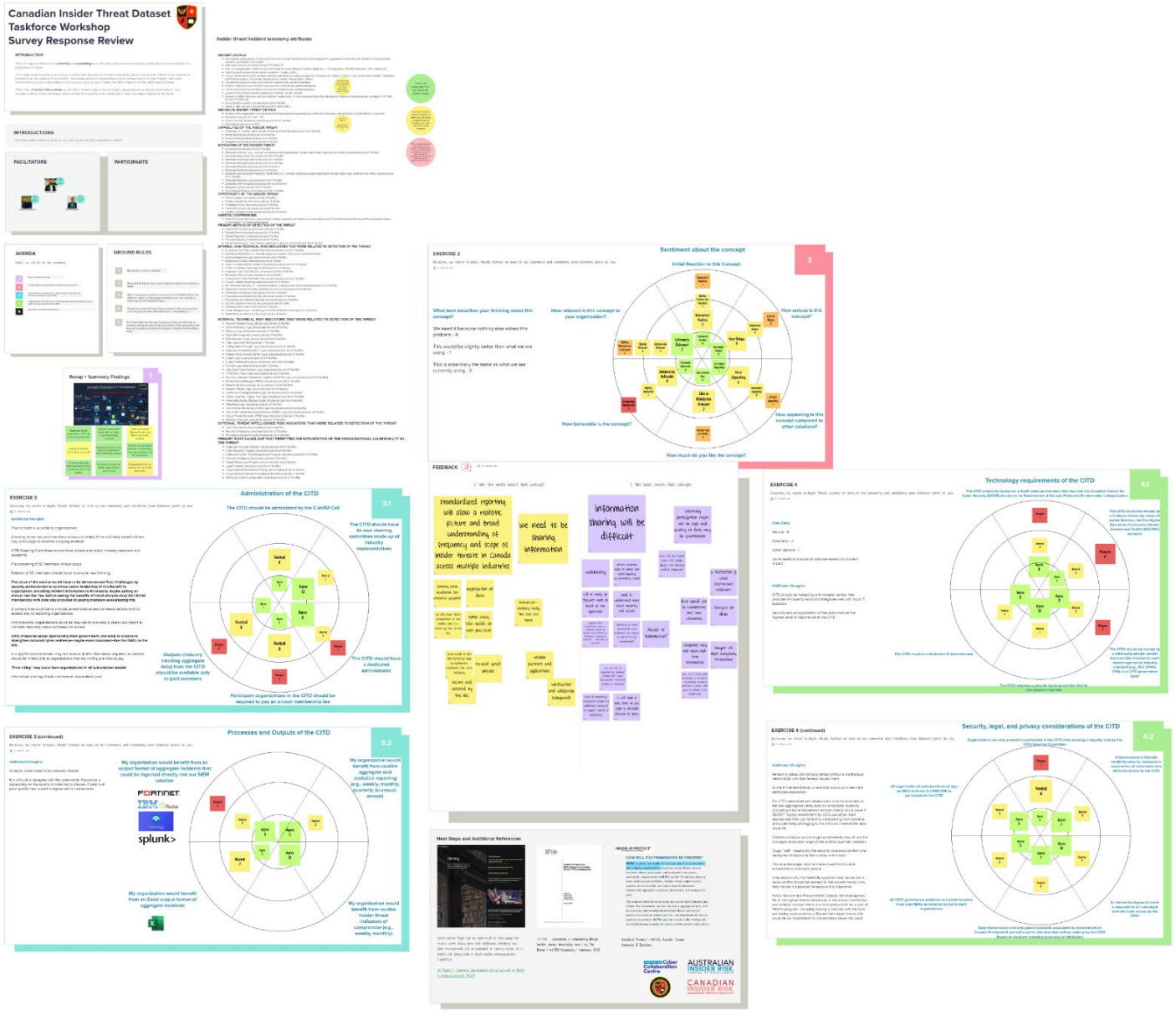
The Canadian Insider Risk Management Centre of Excellence (C-InRM CoE) approached and socialized the concept of a national information sharing initiative focused on establishing a centralized repository of insider threat incidents with Canadian organizations beginning in October 2022. The concept would include a secure data intake and transmission solution for insider threat incidents, with aggregate incident attributes and reporting available to a closed and trusted community of private, public, and academic partners. The outcomes over year one of the initiative would include defining an incident taxonomy for reporting insider threat attacks, developing and refining a concept for an aggregate incident repository for research, policy and program building, and threat mitigation, and establishing the parameters for the governance, policies, and operations of a CITD initiative.



Participants from over 10 Canadian organizations representing academia, communications and information technology, energy and utilities, finance, government, public safety, and transportation sectors offered their thought leadership on a pilot solution to address the incident dataset gap for research and industry mitigation purpose. A taskforce was formalized in July 2023, and a structured survey was sent out in August 2023 for participants to complete.

A facilitated workshop under Chatham House rules was held with taskforce members in September 2023. Responses were reviewed in terms of: 1)

quantitative frequency analysis relating to different aspects of the CITD concept, followed by: 2) a review of members' specific written feedback. Minority, divergent and outlying views were discussed, with the caveat that a proposed CITD solution would likely be architected based on the majority view that would best serve the Canadian community at large.



GENERAL FINDINGS

DISCUSSION

- General sentiment about the CITD concept
  - The CITD concept is on target to meet industry needs and requirements for incident data sharing.
  - The CITD concept could be discussed in partnership with other robust Canadian information sharing solutions that are presently available in the market and involve the collaboration of the private and public sectors (the Canadian Cyber Threat Exchange was specifically mentioned). There was also consideration for the CITD to potentially be a spoke within a hub-based solution at Carnegie Mellon in the U.S., which has for the past two decades, an established U.S.-focused insider threat incident dataset; however, these non-Canadian initiatives may provide limited accessibility and insight to the Canadian practitioner community at large.
  - Information sharing will be difficult—organizations voluntarily being proactive and uploading anonymized, non-personally identifiable information (PII) at first will be limited, but potentially more robust as the initiative evolves. Real-time data sharing will likely not be feasible.
  - Some incident data attributes will be difficult for organizations to obtain as incident management responsibility is shared between multiple teams, on a need-to-know basis (cyber, human resources, information technology, legal, privacy, security), and there may not be a dedicated insider risk management information sharing centralized hub in organizations.
  - Data security, protection from access to information legislation and the inadvertent disclosure of information is paramount. Employing standards such as security controls for Government of Canada Protected B information categorization and ISO 27001 information security risk management, along with independent third-party auditing are critical. As well, additional assurances on protection from access to information legislation for incidents that are

voluntarily shared under critical infrastructure protection provisions will be required.
- The necessary funding to support an ongoing initiative and ensure continuity is an outstanding question. Sources such as government research grants, sponsorship from the private sector, and CITD membership fees, were considered and discussed.

❖ Insider threat incident attributes (incident reporting taxonomy)
- Generally, the taskforce felt that the attributes (see ANNEX A) represented an exhaustive list and was relevant for insider threats.
- There was concern about whether organizations would be able to report all the attributes on a regular basis, and consideration was given to if different attributes should be prioritized, with some identified as mandatory.
- Fulsome information sharing will be dependent on organizations' level of trust in the inherent operations and processes associated to the CITD.
- Through the use of data masking, tokenization, and/or encryption, organizational IDs associated to incidents could be used, and the risk of data being associated to a reporting organization with the implementation of these controls would be minimal in the event of a data breach.
- Incident reporting could be structured against the list of established Canadian critical infrastructure sectors and sub-sectors outlined by Public Safety Canada[i].
- Demographics such as age and sex were suggested as less important[ii]; what is more valuable for threat and risk modelling are insider threat tenure with the organization, skills sets, type of insider threat (malicious vs. negligent), and the root cause individual motivation "triggering" event that led to a compromise (see Annex A).

❖ Administration of the CITD
- Participation in the CITD should be limited to a closed, trusted community of vetted participants.

- Access based on paid membership is an outstanding question. While paid memberships are not necessarily the solution, logistically, the organization administering the CITD must be sustained with a viable source of funding, based on federal government grants or industry contributions to fund at minimum, the positions of dedicated IT administrator and/or program coordinator. There was consideration that entry-requirements should not be prohibitive to the participation of small- and medium-sized organizations.
- An industry-based steering committee dedicated to the oversight of the dataset would be required.

❖ Processes and outputs of the CITD
- Canadian organizations would benefit from more reporting, and situational awareness of insider threat incidents in their respective sectors, as well as in the Canadian environment in general. This reporting may come in the form of raw incident attributes including indicators of compromise, as well as trend reporting.
- While a majority of respondents indicated utility in outputs that could be directly ingested into present industry-standard SIEM solutions, an output of structured data in an Excel format would also be of value.
- What is of key importance is ensuring data quality based on incident taxonomy and also comprehensive reporting to ensure an accurate understanding of the threat environment.

❖ Technology requirements of the CITD
- There is more variation in agreement on a technology platform. The main options discussed were: 1) Government of Canada (GoC) Protected B assessed, 2) Canadian academic, and other 3) third-party private sector infrastructure-as-a-service (IaaS) and software-as-a-service (SaaS) solutions.
- There was consideration that GoC cloud approved hosted solutions for Protected B data with major technology vendors (e.g., Amazon, Google, Microsoft) would also incorporate a significant maturity of security and continuity controls, as well as robust IT administration,

and may be a good starting point given the sensitivity of CITD data based on what is proposed for data capture (i.e., similar to GoC Protected B).
  - Respondents indicated preference for a manual upload of incident data that could be Excel-based onto a secure cloud platform; however, direct outputs from major SIEM platforms are a consideration as well.

- Security, legal, and privacy requirements of the CITD
  - Due to the anonymity of the data and what was outlined for reporting in the proposed insider threat incident taxonomy, the group determined that there were minimal privacy concerns.
  - Respondents were neutral about the requirement for organizations being allowed to participate in the CITD after passing a majority vote by a CITD Steering Committee.
  - Only half of respondents agreed with the requirement for a GoC reliability clearance for all individuals to access the CITD. The other half of respondents were neutral.
  - There is strong consensus on a criminal background verification being required for individuals accessing the CITD.
  - Data transmission and encryption standards equivalent to the protection of GoC Protected B data may be sufficient for the data that will reside in the CITD (based on the insider threat incident taxonomy). However, there should be strong consideration for periodic review and control enhancement based on advances occurring in quantum computing-based attacks.
  - There was a strong consensus on all CITD governance positions and administrators to sign non-disclosure agreements (NDAs). Further, there was a stronger consensus that these positions should also be screened to a GoC standard of Level II-Secret; however, obtaining a federal clearance represents challenges for all parties in terms of additional administrative cost and effort from the sponsoring federal organization, as well as additional administrative overhead when previously screened individuals move out of their positions.
  - There was strong agreement that all organizational participants must sign an MOU to participate in the CITD.

ANNEX A – INSIDER THREAT INCIDENT TAXONOMY
(Structured response formatting based on **CATEGORY** -> Attribute)

INCIDENT DETAILS

- Anonymized organizational ID (structured pick-list of unique identifiers that will be assigned to organizations when they join, identifier will be generated randomly, and master list encoded)
- Date of occurrence (structured format YYYY-MM-DD)
- Size of the organization (structured pick-list of options using Statistics Canada categories: <100 employees, 100-499 employees, 500+ employees)
- Industry (structured pick-list of options: academic, private, public)
- Critical Infrastructure Sector (multiple selections permitted in a structured pick-list of Energy and Utilities, Finance, Food, Government, Health, Information and Communications Technology, Manufacturing, Safety, Transportation, Water)
- Critical Infrastructure Sub-Sector (multiple selections permitted in a structured pick-list of sub-sectors for each of: Energy and Utilities, Finance, Food, Government, Health, Information and Communications Technology, Manufacturing, Safety, Transportation, Water)
- City (structured pick-list that is sourced from a periodically updated database)
- Province (structured pick-list that is sourced from a periodically updated database)
- Country (structured pick-list that is sourced from a periodically updated database)
- Location of occurrence (structured pick-list of options: on-site, remote)
- Duration of attack (structure pick-list of options, single event, or, over a period of time that will allow the selection of beginning and end dates YYYY-MM-DD to YYYY-MM-DD)
- Occurred at third-party? (structured pick-list of Yes/No)
- Before or after job loss? (structured pick-list of Before/After)

INDIVIDUAL INSIDER THREAT DETAILS

- Gender (see Endnote ii)
- Position in the organization (structured pick list of executive/management/sole-contributor/third-party, with definitions of each offered in hyperlink)
- Time in the organization (structured numeric pick-list for years)
- Known criminal background (structured pick-list of Yes/No)
- Type of insider threat (malicious, negligent, accidental)
- Formal education and credentials (pick-list of high school diploma, college diploma, undergraduate degree, graduate degree, professional post-graduate certificate, technical certificate)
- Nationality at birth (pick-list of nation-states)

CAPABILITIES OF THE INSIDER THREAT

- IT training (i.e., coding, cyber security, system architect) (structured pick-list of Yes/No)
- Military training (structured pick-list of Yes/No)
- Security training (structured pick-list of Yes/No)
- Weapons training (structured pick-list of Yes/No)

MOTIVATION OF THE INSIDER THREAT

- Accidental (structured pick-list of Yes/No)
- Deliberate-Coercion (e.g., criminal, competing private organization, foreign nation state, listed terrorist entity) (structured pick-list of Yes/No)
- Deliberate-Disgruntled (structured pick-list of Yes/No)

- Deliberate-Espionage (structured pick-list of Yes/No)
- Deliberate-Ideological (structured pick-list of Yes/No)
- Deliberate-Political (structured pick-list of Yes/No)
- Deliberate-Profit (structured pick-list of Yes/No)
- Deliberate-Recruited and Planted by Third-Party (e.g., criminal, competing private organization, foreign nation state, listed terrorist entity) (structured pick-list of Yes/No)
- Deliberate-Religious (structured pick-list of Yes/No)
- Deliberate-Self-motivated (structured pick-list of Yes/No)
- Negligence (structured pick-list of Yes/No)
- Psychological Distress (structured pick-list of Yes/No)

OPPORTUNITY OF THE INSIDER THREAT

- IT Administrator (structured pick-list of Yes/No)
- Position of Authority (structured pick-list of Yes/No)
- Privileged Access (structured pick-list of Yes/No)
- Third-Party Access (structured pick-list of Yes/No)
- Trusted Custodial Access (structured pick-list of Yes/No)

ASSET(S) COMPROMISED

- Select the assets that were compromised (multiple selections permitted in a structured pick-list of Facilities/Systems/Equipment/Personnel/Information-IP/Information-PII/Finances/Reputation)

PRIMARY METHOD OF DETECTION OF THE THREAT

- Employment Screening (structured pick-list of Yes/No)
- External Reporting (structured pick-list of Yes/No)
- Internal Reporting (structured pick-list of Yes/No)
- Physical Endpoint (structured pick-list of Yes/No)
- Virtual Endpoint (e.g., host, network, application, devices) (structured pick-list of Yes/No)

INTERNAL NON-TECHNICAL RISK INDICATORS THAT WERE RELATED TO DETECTION OF THE THREAT

- Acceptable Use Policy Violation Records (structured pick-list of Yes/No)
- Anonymous Reporting (i.e., security suspicious incident) (structured pick-list of Yes/No)
- Asset Management Logs (structured pick-list of Yes/No)
- Background Checks (structured pick-list of Yes/No)
- Code of Conduct/Ethics Violation Reporting (structured pick-list of Yes/No)
- Conflict of Interest Reporting (structured pick-list of Yes/No)
- Corporate Credit Card Records (structured pick-list of Yes/No)
- Disciplinary Records (structured pick-list of Yes/No)
- Financial and Credit Verification Records (structured pick-list of Yes/No)
- Foreign Contacts Reporting (structured pick-list of Yes/No)
- HR Personnel Records (i.e., employee relations, interpersonal conflict) (structured pick-list of Yes/No)
- Intellectual Property (IP) policy violation records (structured pick-list of Yes/No)
- Performance Evaluations (structured pick-list of Yes/No)
- Physical Access Reader Records (structured pick-list of Yes/No)
- Physical Security Violation Records (structured pick-list of Yes/No)
- Security Clearance Records (structured pick-list of Yes/No)
- Substance Abuse (structured pick-list of Yes/No)
- Threat Intelligence (i.e., monitoring of the Dark Web) (structured pick-list of Yes/No)
- Travel Reporting Records (structured pick-list of Yes/No)

INTERNAL TECHNICAL RISK INDICATORS THAT WERE RELATED TO DETECTION OF THE THREAT

- Account Creation Logs (structured pick-list of Yes/No)
- Active Directory Logs (structured pick-list of Yes/No)
- Antivirus Logs (structured pick-list of Yes/No)
- Application Logs (structured pick-list of Yes/No)
- Authentication Logs (structured pick-list of Yes/No)
- Chat Logs (structured pick-list of Yes/No)
- Configuration Change Logs (structured pick-list of Yes/No)
- Data Loss Prevention (DLP) Logs (structured pick-list of Yes/No)
- Domain Name System (DNS) Logs (structured pick-list of Yes/No)
- E-mail Logs (structured pick-list of Yes/No)
- E-mail Sentiment Analysis (structured pick-list of Yes/No)
- Firewall Logs (structured pick-list of Yes/No)
- Help Desk Ticket System Logs (structured pick-list of Yes/No)
- HTTP/SSL Proxy Logs (structured pick-list of Yes/No)
- Intrusion Detection/Prevention System (IDS/IPS) Logs (structured pick-list of Yes/No)
- Mobile Device Manager (MDM) (structured pick-list of Yes/No)
- Network Monitoring Logs (structured pick-list of Yes/No)
- Network Packet Tags (structured pick-list of Yes/No)
- Permission Change Monitor Logs (structured pick-list of Yes/No)
- Printer, Scanner, Copier, Fax Logs (structured pick-list of Yes/No)
- Removable Media Manager Logs (structured pick-list of Yes/No)
- Telephone Logs (structured pick-list of Yes/No)
- User Activity Monitoring (UAM) Logs (structured pick-list of Yes/No)
- User Entity and Behavioural Analytics (UEBA) Logs (structured pick-list of Yes/No)
- Virtual Private Network (VPN) Logs (structured pick-list of Yes/No)
- Wireless Spectrum (structured pick-list of Yes/No)

EXTERNAL THREAT INTELLIGENCE RISK INDICATORS THAT WERE RELATED TO DETECTION OF THE THREAT

- Law Enforcement (structured pick-list of Yes/No)
- Security Intelligence (structured pick-list of Yes/No)
- Third-party private firm (structured pick-list of Yes/No)

PRIMARY ROOT CAUSE GAP THAT PERMITTED THE EXPLOITATION OF THE ORGANIZATIONAL VULNERABILITY BY THE THREAT

- Corporate Security Program (structured pick-list of Yes/No)
- Cyber Security Program (structured pick-list of Yes/No)
- Dedicated Insider Risk Management Program (structured pick-list of Yes/No)
- External Intelligence (structured pick-list of Yes/No)
- Human Resources Program (structured pick-list of Yes/No)
- Legal Program (structured pick-list of Yes/No)
- Organizational Awareness/Training (structured pick-list of Yes/No)
- Organizational Policies/Procedures (structured pick-list of Yes/No)
- Technical Control Configuration (structured pick-list of Yes/No)

AFTER-ACTION CONTROL REMEDIATION (NOT ORIGINALLY INCLUDED IN THE INCIDENT TAXONOMY, AND IDENTIFIED AS NECESSARY AFTER FURTHER CONSULTATION WITH TASKFORCE)

- Access control (structured pick-list of Yes/No)
- Background screening (structured pick-list of Yes/No)
- Employee/member referred to psychological counselling (structured pick-list of Yes/No)
- Employee/member prosecuted (structured pick-list of Yes/No)
- Employee/member reprimanded in writing (structured pick-list of Yes/No)
- Employee/member terminated (structured pick-list of Yes/No)
- Data loss prevention (DLP) tools (structured pick-list of Yes/No)
- Data segmentation (structured pick-list of Yes/No)
- Forensic capabilities (structured pick-list of Yes/No)
- Incident response protocols (structured pick-list of Yes/No)
- Local/provincial police force notified (structured pick-list of Yes/No)
- Organization exit procedures for departing employees (structured pick-list of Yes/No)
- Physical security (structured pick-list of Yes/No)
- Psychological counselling set as a condition of continued employment (structured pick-list of Yes/No)
- Royal Canadian Mounted Police (RCMP) / Canadian Security Intelligence Service (CSIS) / Communications Security Establishment (CSE) notified or involved (structured pick-list of Yes/No/Unknown)
- Routine auditing (structured pick-list of Yes/No)
- Third-party contracts and agreements (structured pick-list of Yes/No)
- Training and awareness programs (structured pick-list of Yes/No)
- Use of two-factor authentication (2FA) (structured pick-list of Yes/No)
- User activity monitoring systems (structured pick-list of Yes/No)
- User behaviour analytics (structured pick-list of Yes/No)
- Whistleblower policies (structured pick-list of Yes/No)
- *For employees/members with Treasury Board Secretariat (TBS) reliability and/or security clearances, was a security waiver administered? (structured pick-list of Yes/No)
- *For employees/members with Treasury Board Secretariat (TBS) reliability and/or security clearances, was clearance downgraded? (structured pick-list of Yes/No)
- *For employees/members with Treasury Board Secretariat (TBS) reliability and/or security clearances, was clearance revoked? (structured pick-list of Yes/No)

Endnotes

[i] https://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/esf-sfe-en.aspx
[ii] While there is no information in the present insider risk management literature indicating a correlation between gender and the propensity to act maliciously, it could prove useful as a metric to inform security practitioners and managers in terms of limiting gender bias in the evaluation of insider threats. Metrics focused on gender could include the full range of gender identities. While this is a sensitive matter, a reporting organization could be further given the option to not answer this question, indicate that the data is not being collected, or that it is unknown.