IN THE MATTER OF AN ARBITRATION

BETWEEN

HYDRO ONE INC.

("Hydro One" or the "Employer")

and

POWER WORKERS' UNION

(the "PWU" or the "Union")

GRIEVANCE: HO-P-157
Re: Reliability Screening Procedure

CHIEF ARBITRATOR: John Stout

APPEARANCES:

For Hydro One:
Daniel McDonald - Norton Rose Fulbright Canada LLP
Eugene Kosziwka – Manager, Labour Relations
Alex MacKenzie – Director, Labour and Employee Relations
Sharon Bharat – Manager Workforce Screening
Eddie Ng – Vice President, Security & Infrastructure
Andrew Chester – President and CEO, Juno Risk Solutions Inc.
Camilla Zienkiewicz – Labour Relations Consultant

For the PWU:
Donald K. Eady - Paliare Roland LLP
Kate Shao - Paliare Roland LLP
Jessica Latimer – PWU General Counsel
Christa Helsdon – PWU Staff Officer
Darren Nesbitt – PWU Sector VP
Andy Fritsch – PWU Sector Rep
Rodney McLeod – Chief Steward
George Harrison – Chief Steward

HEARINGS HELD IN TORONTO, ONTARIO ON NOVEMBER 6, 2025

AWARD

Introduction

[1] This matter concerns a January 17, 2023 policy grievance (HO-P-157) filed by the PWU alleging that Hydro One's Reliability Screening Procedure (SP 1975) (the "Policy" or "Procedure") is overly broad, unreasonable, and in breach of the Collective Agreement and the *Personal Information Protection and Electronic Documents Act*, SC 2000, c.5 ("*PIPEDA*").

[2] The parties signed a side letter during 2023 collective bargaining, which addresses security clearances (the "2023 Side Letter"). This Side Letter provides as follows:

> **<u>This side letter will be subject to the outcome of P-157</u>**
>
> April 1, 2023
>
> Mr. Tom Chessel
> Vice President, Sector 3
> Power Workers' Union
>
> **RE: SECURITY CLEARANCES**
>
> This side letter is not to be reproduced in the collective agreement. The PWU acknowledges and agrees that the Employer has the right to perform appropriate Personal Risk Assessments (PRA) on existing, regular, temporary and Appendix A employees when required for legal or regulatory reasons. Where the Employer has reasonable cause to remove an employee from his/her position as a result of an employee's inability to pass a PRA, the employee will be transferred to an equivalent position for which a PRA is not required with no loss of salary. An "equivalent position" is one that is reasonably similar to the job the employee is doing, taking into account both the classification and location of the job.
>
> While the PRA process outlined above will continue in the immediate future, the Employer is currently reviewing its workforce screening practices. The parties agree to meet within 90 days of ratification to review potential new screening protocols for PWU represented regular, temporary and hiring hall employees.

[3] The 2023 Side Letter acknowledges and agrees that Hydro One has a legal or regulatory requirement to perform a Personal Risk Assessment ("PRA") pursuant to requirements established by the North American Electric Reliability Corporation ("NERC"). These requirements are found in NERC's Critical Infrastructure Protection ("CIP") standards (the "NERC Standards"). The 2023 Side Letter provides for an accommodation of sorts for those employees who are unable to pass a PRA. The 2023 Side Letter goes on to acknowledge that Hydro One was reviewing their screening practices and the parties would meet to review potential new screening protocols for PWU represented employees. The parties were unable to reach an agreement with respect to the appropriate screening protocols for different classifications, which are found in the Policy. As a result grievance HO-P-157 was referred to me as Chief Arbitrator for resolution.

[4] The PWU points out that all Hydro One employees are subject to the Policy and they are all screened at one of three levels every seven years. The PWU submits that each screening level exceeds the NERC Standards, including a criminal records check, driver's abstract, credit report and other screening tools without regard to the nexus between employee functions and related risks. According to the PWU, nearly 70% of the PWU members at Hydro One undergo credit report checks and other checks, and unnecessarily intrusive resolution of doubt interviews are held at Hydro One's discretion.

[5] The PWU does not dispute the applicability of the NERC Standards to some of Hydro One's workforce. While there is a reasonable basis for a policy to adhere to the NERC Standards, the PWU disputes the reasonableness of Hydro One's Policy as follows:

a. The breadth of the Policy beyond those subject to the NERC standards (including subjecting all PWU members to regular criminal records checks). In other words, Hydro One is using the NERC standards as a springboard to attempt to authorize additional checks for employees who have no unescorted access to physical or cyber assets of the Bulk Electricity System ("**BES**");

b. The credit report checks required at Level 3 (impacting nearly 70% of the PWU bargaining unit at Hydro One);

c. The driver's abstracts required, especially for those who do not drive as part of their regular work duties or where there are no safety concerns; and

d. The scope of the resolution of doubt interviews held by Hydro One.

[6] The PWU does not take issue with the applicability of the Policy to new hires or non-PWU members. The PWU acknowledges that such matters fall outside the Collective Agreement. Therefore, the focus of this matter is restricted to Hydro One employees who are PWU members.

[7] The PWU argues that the security clearance requirements under the Policy infringe upon employee privacy rights without properly balancing the degree of risk and the degree of intrusion. The PWU submits that balancing in this case demands less intrusive measures. The PWU therefore seeks an amendment to the Policy that would exclude those not subject to the NERC standards, the removal of the credit report checks, driver's abstracts, other checks as set out in the Policy and implementing parameters around the resolution of doubt interviews.

[8] Hydro One takes the position that the grievance is without merit and ought to be dismissed. Hydro One asserts that they have a statutory duty to protect the public interest regarding the adequacy, safety and reliability of their electricity transmission and distribution business. Hydro One submits that as a critical infrastructure organization, they are subject to heightened security risks, and they have a right to take reasonable measures to uphold their statutory and regulatory obligations.

[9] Hydro One insists that the Policy is consistent with regulatory standards and governmental guidance, striking an appropriate balance between the privacy rights of employees and Hydro One's interests and obligations to ensure the safety and security of the electricity grid, their other assets and their employees.

[10] Hydro One submits that the Policy screens persons who pose a risk to Hydro One staff, safety and the integrity of the electrical grid as well as Hydro One's intellectual property. The Policy acts as a critical safety control against fraud, theft in the workplace, violence or workplace violence harassment, sabotage and espionage. Hydro One argues that to weaken the Policy as argued by the PWU, poses a serious security and safety risk to other employees, the public and national security.

[11] After carefully considering the parties submissions, and for reasons that follow, I find that the Policy is overly broad and unreasonable. The Policy infringes upon all employees' privacy rights and does not provide a balanced approach. The evidence presented does not reflect a general problem in the workplace that would justify invading the privacy of all employees in a manner provided for in the Policy. Moreover, I am not satisfied that Hydro One has exhausted less intrusive alternatives measures for addressing the risk. Therefore, I am allowing the grievance.

Process and submissions prior to arbitration

[12] The grievance originally came before me at the scheduled monthly mediation/arbitration hearing on October 2, 2023 for mediation. The parties filed brief submissions in advance of the mediation. At that time, the PWU indicated a willingness to work with Hydro One to determine the appropriate security clearances required for specific job classifications. Hydro One maintained their position that the grievance was without merit, but they were willing to engage in meaningful discussions to find a resolution.

[13] The matter was brought back on November 9, 2023, but adjourned so that Hydro One could provide a chart with PWU represented roles, screening level and explanatory notes for the PWU to review. The goal was to attempt to find common ground on the PWU members who would be subject to different levels of security clearances.

[14] The matter was brought back before me as a touch point on April 16, 2024. By this time, Hydro One had provided the PWU with a spreadsheet outlining the PWU represented employees subject to Level 1 and Level 2 screening procedures. This information was in addition to a previous document Hydro One provided to the PWU indicating those PWU represented employees subject to Level 3 screening. As such, the PWU had a list of all their members who were subject to the Policy's three levels of screening.

[15] The PWU recognized Hydro One's obligation to meet the NERC requirements to implement a risk assessment program for those with "authorized cyber or authorized unescorted physical access to Critical Cyber Assets." The PWU pointed out that the Hydro One documentation went beyond the NERC requirements and subjected all PWU members to reliability screenings. The PWU maintained that employees screened at Level 1 and 2 either had no access or non-critical access to critical cyber assets. They questioned how many of these employees may have access to Hydro One's "critical cyber assets." The PWU took the position that Hydro One ought to be able to compartmentalize various systems to limit access to employees who do not require access as part of their positions.

[16] The PWU maintained that the list of positions at the highest level of screening (Level 3) was overly broad (69% of their members) and not tied to the NERC requirements.

[17] In addition, the PWU had privacy concerns about the requirement to provide a driver's abstract for employees who did not operate Hydro One vehicles and the credit report requirement. The PWU also raised concerns related to the requirement to provide three references.

[18] As part of my monthly award, I issued a direction to the parties on April 16, 2024. The direction noted the parties agreement to exchange additional information to provide for more fulsome discussions and a path towards a possible settlement of the dispute. Hydro One was to provide the PWU with the additional

information by June 5, 2024 (the date was extended by agreement to June 7, 2024).

[19] On June 7, 2024, Hydro One provided the additional information referenced in my direction. Hydro One maintained that reliability screening must occur for all potential and current employees. Hydro One was agreeable to amending the Policy to expressly contemplate the PWU's right to grieve an alleged unreasonable application of the screening process or procedures.

[20] The matter was brought back before me on April 14, 2025. In my April 21, 2025 monthly award I directed the PWU to identify levels of screening that they viewed as being reasonable. The PWU responded on May 13, 2025, providing a proposal for two screening levels; NERC and non-NERC PWU members. Hydro One maintained their position on the reasonableness of their Policy.

[21] Hydro One provided supplementary submissions on August 5, 2025.

[22] The grievance proceeded to arbitration on November 6, 2025. Prior to the hearing, the parties filed extensive written briefs (the "Briefs"). The PWU's Brief referenced material from Ontario Power Generation ("OPG"). Hydro One raised an objection to the material being filed and OPG sought to intervene, objecting to the inclusion of a document that they considered confidential. The PWU agreed to remove the confidential document, and they filed an amended Brief.

[23] The Briefs filed prior to the hearing also referred to earlier submissions that had been filed. I directed the parties to each file a "compendium", which was to include all material that they wanted me to review before issuing my award. Hydro One's compendium was filed on November 17, 2025 and it included additional material based on my inquiries during the hearing. This material included information relating to Hydro-Québec's screening process and Nova Scotia Power ransomware attack. The PWU responded to this additional material on December 18, 2025.

Background Facts and evidence submitted by the parties

[24] Hydro One is a successor corporation to the former Ontario Hydro. In 1998 Ontario Hydro was broken into several companies, including Hydro One, OPG, the Electrical Safety Authority (ESA), and the Independent Electricity System Operator (IESO) pursuant to the *Electricity Act, 1998*, S.O. 1998, c.15, Sch A (the "*Electricity Act*").

[25] Hydro One is Ontario's largest electricity transmission and distribution utility. Hydro One distributes electricity across the province to approximately 1.5 million predominantly rural customers, or approximately 26% of the total number of customers in Ontario.

[26] Hydro One is regulated pursuant to the *Electricity Act*, see Part IV, section 48.1, which provides that Hydro One must operate its facilities and distribution systems in communities in accordance with such conditions and restrictions as may be prescribed by regulation.

[27] The PWU represents the majority of unionized employees of Hydro One. The Society of United Professionals (the "Society") represents other unionized employees working for Hydro One. The employees represented by the PWU include both "Regular" employees and Appendix "A" hiring hall employees.

[28] The collective bargaining relationship between Hydro One and the PWU is very mature, dating back to the days of Ontario Hydro.

[29] The most recent Collective Agreement was resolved during collective bargaining on May 5, 2025 for an agreement between October 1, 2025 and March 31, 2028. The 2023 Side Letter was renewed during this recent set of negotiations.

The Statutory Framework

[30] Hydro One is required to adhere to Market Rules for the Ontario Electricity Market (The "Market Rules") and reliability standards established by NERC and other applicable standards authorities.

[31] NERC is a not-for-profit international regulatory authority, whose mission is to assure the effective and efficient reduction of risks to the reliability and security of the electricity grid.

[32] The NERC Standards apply to North American entities that own or manage facilities part of the US and Canadian electric power grid. The NERC CIP framework establishes reliability standards to safeguard the North American electricity grid from cyber and physical security threats, with the aim of ensuring uninterrupted power supply across the continent.

[33] The NERC Standards are incorporated domestically through provincial legislation. In Ontario, that is done through the *Electricity Act*, which defines the NERC as a "standards authority", who is authorized to create reliability standards (s. 36.2). In addition, s. 32(1)(c) of the *Electricity Act* grants the IESO with authority to make rules establishing and enforcing standards and criteria relating to electricity supply. It is through these legislative grants that the applicable NERC standard, CIP-004-6 (Cyber Security – Personnel & Training), applies.

[34] The CIP-004-6 (Cyber Security – Personnel & Training) standard requires entities, like Hydro One, to establish a PRA program for **"all personnel who are granted authorized electronic access and/or authorized unescorted physical access to its BES Cyber Systems"** (emphasis added).

[35] The NERC Standard does not apply to every employee of companies like Hydro One. Under the NERC standard, an employee who simply has access to Hydro One's computer system or an employee who has physical access to Hydro

One facilities, which are not part of the BES Cyber Systems would not require a PRA screening.

[36] The PRA screening program under the NERC Standard must include:

- Identity verification; and
- Seven-year criminal history check.

[37] The NERC Standard also permits more detailed reviews, "as permitted by law and subject to existing collective bargaining unit agreements, depending upon the criticality of the position." The NERC Standard also requires an updated PRA every seven (7) years for those persons covered by the Standard.

[38] Prior to the introduction of the Policy, Hydro One had a PRA program that complied with the NERC Standard. The NERC Standard PRA screening was the only form of reliability screening or security clearance conducted on existing employee's at Hydro One.

The 2015 incident and Juno Risk

[39] Hydro One filed an April 8, 2025 will say of Andrew Chester, along with supporting documentation. Mr. Chester is the Chief Executive Officer of Juno Risk Solutions ("Juno Risk"). Mr. Chester was an intelligence officer with the Royal Canadian Navy for 20 years prior to forming Juno Risk. Mr. Chester has a law degree from the College of William and Mary and is licensed to practice law in the Commonwealth of Virginia.

[40] Mr. Chester's will say is extensive and it outlines a number of areas, including the events that precipitated Juno Risk's engagement by Hydro One. Mr. Chester also provides his views and opinions about reliability screening.

[41] Juno Risk has been in business since 2010, and they are a boutique risk management consulting firm with a specialized practice in investigations of

wrongdoing, harassment and violence in the workplace. They also have a practice area that focuses on insider risk management and workforce reliability screening.

[42] According to Mr. Chester, in the Fall of 2015, Hydro One was approached separately by both the Canadian Security Intelligence Service (CSIS) and the Royal Canadian Mounted Police (RCMP) about an active investigation underway regarding a former Co-op student who was acting as a mid-level ISIS recruiter while employed at Hydro One. This individual was subsequently killed while in a Middle Eastern country where he was responsible for the ISIS drone program.

[43] After concluding their own internal investigation, Hydro One retained Juno Risk to conduct a separate national-security focused investigation of the incident. During the review of the Co-op student's hiring-related documents, certain "red flags" were identified. Mr. Chester noted that at the time Hydro One screened applicants for role suitability and not for reliability.

[44] Mr. Chester advises that he recommended that Hydro One implement a workforce screening program focused on reliability to identify and mitigate the risk associated with the ISIS-related case. Juno Risk also recommended that Hydro One's workforce screening program should be tailored to address a full range of risk management responsibilities, including national security threats, workplace harassment and safety issues, amongst other risks.

[45] Hydro One directed Juno Risk to design a workforce screening program that would be the means to detect job applicants that may pose a risk to Hydro One.

[46] Mr. Chester refers to a May 2016 benchmark study of several "peer organizations" that Juno Risk conducted and is titled *Leveraging Data: Reducing Risk*. The six electricity sector companies who contributed to the benchmark study included BC Hydro, Capital Power, Emera, Brookfield, OPG and Hydro Québec. The Executive Summary notes that the only regulatory requirement under NERC

is for criminal records check every seven years, for the subset of employees requiring access to critical cyber assets. It is noted that universally the participants went beyond the NERC requirement. According to the study, all participants screened all employees with a criminal background check, and other screening tools were used in varying degrees.

[47] I note that the benchmark study indicates that unions were 100% on board and supported the screening process. However, the study does not provide any useful details of the actual screening programs that have been implemented and what types of screening protocols the unions agreed to with the six employers. The PWU represents employees at OPG and they advise that OPG does not have as broad a program as Hydro One's Policy. The study does not specifically address the issues in this matter involving the levels of screening, and the types of screening applicable to various employees. This makes it very difficult to assess the weight, if any, to give to this document.

The internal "Steering Committee"

[48] Mr. Chester indicates that an internal "Steering Committee" at Hydro One was created and Juno Risk acted as the committee's secretariat. The Steering Committee made an early decision to screen all staff members. The program would begin with new hires, then extend to third-party contractors and ultimately screen all existing employees and have a rescreening component.

[49] Included in the material provided by Mr. Chester are "Decision Briefs" that Juno Risk prepared for Steering Committee consideration. There is a Decision Brief on credit screening and a Decision Brief on driver's abstracts, but they both seem to be tailored towards obtaining information on new-hires and not existing employees.

[50] There is a Decision Brief concerning application of the screening to the existing workforce. The Decision Brief includes a number of options including

grandfathering existing employees. The Decision Brief sets out advantages and disadvantages of the three options. The Decision Brief also references the six benchmarked peers utilizing universal screening. The issue summary provides:

> Hydro One should ensure that the rollout of the screening program is consistent with its organizational culture and avoids potential litigation attempts, while not inadvertently introducing unaccepted risk to the organization, its staff, its customers, and the operation of the grid.

[51] There are also Decision Briefs relating to the "refresh rate" or rescreening employees, which two of six peers do on a five year basis. There is reference to the Government of Canada refreshing Secret and Top Secret clearances on a five year basis.

[52] Mr. Chester explained that the Steering Committee made a conscious and informed decision to exclude the use of vulnerable sector criminal record checks or judicial matters checks in reliability screening. Mr. Chester opined that prior criminal records on their own correlate more thinly to reliability concerns than combinations of other, more dynamic screening tools, such as personal history questionnaires, credit history reports, and driver's abstracts.

The creation of the Hydro One Reliability Standard

[53] Mr. Chester advises that the Hydro One Reliability Standard was initially drafted by him and his staff and is reflective of the design decisions reached by the Steering Committee. The Hydro One Reliability Screening Standard was submitted to Hydro One on June 5, 2016.

[54] Mr. Chester described the three levels of screening that were designed for the Policy.

- **Level 1** screening is the lowest and it is based on the narrowest range of staff risk types. The example provided was an Area Forest Technician who

does not have access to electronic systems but may require unescorted physical access to physical security perimeter (PSP) sites.

- A **Level 2** example position might include Clerical staff who require electronic and cyber system access for their positions and present a risk to using their access for nefarious purposes.

- **Level 3** positions would include those subject to the NERC Standard as well as Stations Support Clerks, who have systems, applications and products SAP data system access, which contains some of the most sensitive business information at Hydro One.

[55] Mr. Chester indicates that he is personally aware of one national security case at Hydro One that involved an employee whose role was primarily focused on SAP access and which he surmised was his interest to compromise for unauthorized purposes. Unfortunately, no additional details were provided, including whether this person was a PWU member, what position the person held with Hydro One and if they had committed any misconduct.

[56] Mr. Chester addresses the fact that there is virtually no limit to the ability of an company to peer into the life of another person using publicly available information, including court records, property and business ownership records, and social media. Personal data is also available for sale in the open market. Mr. Chester indicates that concerns were raised and considered about employee privacy and placing controls to stop overzealous pursuit of information in excess of what was needed to make a reliability decision.

[57] Mr. Chester indicates that he is aware of many cases where staff risks have manifested at various points in the employment lifecycle, including long after the employee was hired. Mr. Chester cited some non-Hydro One examples.

[58] Mr. Chester identifies one Hydro One situation involving a Chinese national who applied for a Hydro One job but was deemed unreliable. The Chinese national candidate’s screening process identified two long-term Hydro One employees with close personal relationships to the candidate. Mr. Chester does

not indicate what, if anything, occurred to these Hydro One employees or if these employees were involved in any malfeasance.

The Privacy Commissioner of Canada investigation of Desjardins

[59] Mr. Chester points to the 2019 Office of the Privacy Commissioner of Canada (OPC) investigation into Desjardins' compliance with *PIPEDA* following a breach of personal information between 2017-2019. The breach involved an existing "malicious employee" of Desjardins who was exfiltrating personal information over a period of 26 months. The OPC concluded that Desjardins contravened *PIPEDA* principles with regards to accountability, retention periods, and security safeguards. The investigation also included recommendations to Desjardins to address the contraventions found.

[60] In their investigation report, the OPC notes that there are both external and internal threats to personal information data stored by Desjardins. The OPC indicates that internal threats may be non-malicious or malicious such as the matter they were dealing with at Desjardins. The OPC then focuses on the following five elements to combat insider threats:

- Security screening and confidentiality agreements
- Organizational policies and procedures
- Employee training and awareness
- Access controls and data segregation
- Oversight and monitoring

[61] The OPC notes that Desjardins had a security screening program in place that focused on both new hires and existing employees that were moving to new positions. For certain employees, security clearances were renewed every five years. Desjardins had screened the malicious employee at the point of onboarding and that check raised no concerns.

[62] The OPC found that Desjardins' security screenings were acceptable and consistent with currently recognized standards and practices (citing ISO 27001 A.7.1.1). The OPC also found that while security screenings are necessary, they are insufficient on their own to combat insider threats. It is noteworthy that the OPC did not take issue with Desjardins security screening or make any recommendations to expand those screenings.

[63] Subsequently, Desjardins on their own behalf revised their security screening protocols, mandating that both screening and credit check procedures would be subject to a three-year renewal period for all employees with high-level access privileges.

[64] The OPC investigation report identifies inadequate protection measures and gaps in the other four elements: policies and procedures; employee training and awareness; access controls and data segregation; and oversight and monitoring.

[65] Mr. Chester provided evidence of a recent national security case involving a long term employee who was granted a PRA clearance in 2020 under the NERC Standard that did not raise any red flags. When suspicions were raised, the Workforce Screening Team then applied elements of the reliability screening process to reveal a number of risk factors and further evidence of wrong doing. Mr. Chester did not identify if this Hydro One employee was a PWU member or any other details relating to this employee.

[66] Mr. Chester states his opinion that the compromise of employees is an increasingly attractive component of cyber penetration strategies. This is why he recommends that reliability screening should go beyond the hiring process. Mr. Chester notes that there are no specific obligations incumbent on Hydro One to adapt to this environment, but sound risk management dictate that threats should be mitigated, where possible.

[67] Mr. Chester indicates that credit checks and driver's abstracts constitute independent checks that serve both to validate self-declared data as well as to independently identify risk factors. The following observations are found in his evidence:

- Rarely are credit checks of value in and of themselves, but can serve to corroborate other screening data, such as addresses or employment history, financial circumstances relative to peers and anomalous transactions or cash flows.
- Credit checks have provided screeners with evidence of undisclosed second employment contrary to the Hydro One *Code of Conduct*.
- Lack of credit information has led screeners to discover through further interviews candidates with undisclosed and significant ties to foreign governments. Inconsistency between self-declarations and credit history reports demonstrate dishonesty.
- A 23-year old co-op student credit report showed a mortgage in excess of one million dollars. The reliability interview established that they were involved in a scheme with their family to commit immigration fraud. They were deemed unreliable.
- Credit checks are according to Mr. Chester less intrusive than an investigation of publicly available information.
- Driver's abstracts provide an excellent supplement to the criminal check and acts as a proxy measure for propensity to abide by authority. Those with criminal records in almost every case have driving offenses.

[68] Mr. Chester provided evidence of a long-standing Hydro One employee who was subject to a PRA as part of a change in role. This employee self-disclosed that they had a prior conviction for murder, which would be found in the criminal record check. Mr. Chester acknowledged that if the screening program had been in place when this employee was hired, he would likely have not been offered a position. However, further investigation revealed that while the offense was terrible, it occurred when the employee was 18 years old. The employee had subsequently trained as an electrician in jail and was a model prisoner. Conversations with the employee's parole officer revealed that the employee had a flawless record since release and was active in youth diversion programs leveraging their own experience to help others. The employee was granted the PRA without reservations.

[69] According to Hydro One, since its inception the program has successfully identified and blocked 41 candidates at varying levels of risk, at least 5 of which were high-risk candidates (including those linked to Chinese and Russian state actors). Additionally, the program has in at least one case, detected the same national security concern that formed the basis of the original 2015 incident that prompted the program.

The Policy

[70] The Policy was introduced by Hydro One in and around 2022 and has been updated several times. Prior to introducing the Policy, "reliability screenings" were facilitated by department and any criminal records checks were done externally at local police authorities. Under the Policy, reliability screenings are conducted internally through Hydro One Corporate Security with the assistance of a third-party Mintz Global Screening. All of the data collected under the Policy is stored in Canada.

[71] The Policy applies to all persons working within Hydro One and its subsidiaries, as well as including third-party contractors. The stated purpose of the Policy is to outline the procedure for obtaining and maintaining "Reliability Status." The Policy also establishes the minimum Reliability Screening requirements for access to Physical Security Perimeters, BES Cyber Systems (BCS), Electronic Access Control or Monitoring Systems (EACMS), Protected Cyber Assets (PCAs), Physical Access Control Systems (PACS), or Electronic Security Perimeters (ESP). It is stated that the Policy is a requirement to meet the NERC Critical Infrastructure Protection (CIP) regulatory obligations. However, it is clear that the Policy goes beyond applying to those employees who have authorized cyber or authorized unescorted physical access to critical cyber assets.

[72] Hydro One acknowledges that NERC CIP regulations mandate background checks for access to BES Cyber systems only, but their Policy goes beyond that to include additional measures beyond compliance with the NERC

Standard. These measures are to address risks associated with system access. Hydro One points out that all forms of network access, including email and internal connectivity, can present potential security vulnerabilities. Background checks help identify possible concerns prior to granting access, thereby lowering the risk of unauthorized activity, data lose or disruption.

[73] Hydro One utilizes the SAP enterprise software system, which is widely deployed by large organizations to manage a range of operations, including finance, human resources, supply chain management, and asset administration. User access to SAP facilitates interaction with critical business data and functions, encompassing financial transactions, payments, confidential information, workflow management and approvals.

[74] According to Hydro One, it is important to recognize that even basic, entry level access to SAP does not equate to negligible risk. Individuals with such access may serve as initial entry points into the environment, potentially enabling malicious activity. By leveraging an initial basic SAP access, a threat actor could incrementally escalate privileges, thereby gaining access to sensitive data, critical applications, or administrative capabilities. As a result, Hydro One is of the view that all levels must be strictly regulated and continuously monitored to mitigate the risk of significant security breaches-both within SAP and across the broader Hydro One organization.

[75] The Policy sets out three levels of Reliability Screening, each corresponding to the level of access an employee has to critical cyber assets or the BES. The three levels are as follows:

- **Level 1 (Physical Access) – applicable to 207 (4%) PWU employees who have no SAP access.**
  Reliability Status includes the following mandatory screening verifications:

  a. Identity Verification
  b. Address Verification (seven-year)

c. Driver's Abstract (record and license verification)
d. Criminal Records Check
e. International Security Verification (International Sanctions and Terrorist Watch Lists)

This is the minimum level of Reliability Screening that will be performed to meet the requirements of the PRA described in the NERC CIP standard requirement CIP-004-R3 – PRA.

Examples of classifications screened at this level include Carpenter, General Helper, Mechanical Journeyperson.

- **Level 2 (Electronic Access)** – **applicable to 1,387 (27%) PWU employees who have non-critical SAP access**
  Reliability Status includes the following mandatory screening verifications:

  a. Level 1 Reliability requirements (as above)
  b. Education Checks
  c. Credentials - Professional Qualifications / Accreditation
  d. Employment History (10 Year Standard)
  e. Reference Checks – Standard Reference
  f. Media Check
  g. Social Media Check

  Examples of classifications screened at this level include Customer Service Representatives (CSO), Lines Customer Support Clerk, Stockkeeper, Provincial Services Clerk, Electrical Forester Labourer Journey, Instructor-Vehicles and Equipment, Truck Driver Class 1, lines Journeyperson; Regional Maintainer, Job Clerk.

- **Level 3 (Sensitive Electronic Access) – applicable to 3,513 (69%) PWU employees with critical SAP access**
  Reliability Status includes the following mandatory screening verifications:

  a. Level 2 Reliability requirements (as above)
  b. Credit Report Check
  c. Reference Checks – Comprehensive Reference

  Examples of classifications screened at this level include Stockkeeper, Meter Technician Trainee, Administrative Assistant, Meter & Relay Quality

Tech, Meter Reader, Planning Scheduling Technician, Regional Maintainer-Lines, Helicopter Pilot

For all levels of Reliability Status, the following additional checks may be conducted as needed:

a. Deep Web Internet Search
b. International Criminal Records Checks (where available)

A reliability interview with the individual may also be used to resolve doubt, address adverse information, or obtain more detail that may be required for a proper determination of reliability.

[76] According to section 1.2.2, individuals may be required to undergo fingerprinting to further confirm their identity in "some rare cases." Individuals are also provided with an opportunity to self-declare any criminal convictions.

[77] Section 1.2.3 lists the factors affecting the inability to complete the Reliability Screening Procedure as follows:

- Type, seriousness, and number of criminal convictions (Appendix B).
- Frequency of criminal convictions (indicating a pattern of behaviour).
- A criminal record that indicates a reasonable suspicion of a threat to the BES Cyber System and/or other electricity sub-sector assets (domestic and/or international terrorism/sabotage).
- Type, seriousness, and number of driving infractions (Appendix E).
- Misleading, deceptive, or false representations made by the individual during the Reliability Screening procedure.
- Not providing authorization for the disclosure of information to Hydro One that is required to complete the Reliability Screening procedure.
- Failing to provide the required documentation.
- Any information uncovered that requires the cessation of the Reliability Screening Process (Appendix G).

[78] Section 1.2.5 precludes pardoned criminal convictions and any convictions under the *Young Offenders Act* from forming a finding of "Deemed Not Reliable":

A criminal conviction for which a pardon has been granted, or any conviction under the Young Offenders Act, will never be considered or form any part of the basis for a "Deemed Not Reliable".

- This procedure may involve consultation with Human Resources, Employee Relations, Legal, and in some instances the Hiring Manager. This is at the discretion of the Chief Security Officer of Hydro One.
- The individual may also be invited to an interview to resolve any apparent inconsistencies or clarify any unusual circumstances.
- This procedure may result in the creation of a Workplace Performance Agreement (WPA), a written document signed by the individual and the Chief Security Officer of Hydro One, which outlines any conditions that the individual must follow to obtain and/or maintain the Reliability Status that is required for their position.

[79] At the end of the screening process, individuals are granted "Deemed Reliable" (successful) or "Deemed Not Reliable" (unsuccessful) statuses. There is a two-stage appeal process involving first the Chief Security Officer, and then the President and CEO of Hydro One (section 1.3).

[80] The Policy does not appear to permit an employee to challenge the screening process or these findings through the grievance and arbitration procedure under the Collective Agreement. There is also nothing in the Policy that would preserve the employee's pay or benefits while the Reliability process and any appeals or grievances are ongoing.

[81] To maintain Reliability Status, employees must renew their screenings every seven (7) years. Contractors must renew every three (3) years. Screenings must be performed again where there is a break in employment or contract of over 365 days (section 1.4).

[82] Individuals may be reassessed further if they become the subject of an investigation into a breach of conduct, criminal act(s), and any other behavior that is inconsistent with their Reliability Status (section 1.6):

> An individual's Reliability Status may be reassessed if the individual becomes the subject of an investigation into a breach of conduct, criminal act(s), or any other behavior that is inconsistent with their Reliability Status. The individual's Reliability Status may be suspended or downgraded immediately, pending the outcome of an investigation. Upon completion of the investigation, the individual's Reliability Status may be suspended, downgraded, or revoked. Any such suspension, downgrade, or revocation of Reliability Status will be at the discretion of the Chief Security Officer. The Chief Security Officer may also set a time period for a temporary suspension or temporary downgrade.

[83] Criminal records under the Policy include convictions, dispositions, discharges, and outstanding entries. This includes charges, warrants, judicial orders, peace bonds, probation, and probation orders (Appendix D, p. 16). Therefore, reliability findings may be made where the judicial process is ongoing and may include warrants and peace bonds.

[84] The information gathered pursuant to the Policy is collected, reviewed and stored in a manner that complies with all applicable privacy legislation. The information is stored by Mintz Global Screening (Mintz) in Canada and in manner that complies with *PIPEDA* and any other relevant legislation.

Application of the Policy and the PWU concerns relating to the levels and employees covered by the Policy

[85] Hydro One advises that since 2018 the screening unit has reviewed many files and of those approximately 85 included evidence of past criminal convictions. Of those files, only one person was not hired. They point to this as evidence of the effectiveness and fairness of the program.

[86] Hydro One advises that they have identified and blocked several high-risk candidates fitting known patterns of espionage from being hired into the Company. Hydro One states that these actors are known to target for recruitment existing employees. They point to a situation where a review of an existing employee identified an agent of ISIS who was engaged in recruitment activities. However, I was not provided details of this individual particularly if the person was a PWU represented employee or if they committed any wrongdoing.

[87] Hydro One acknowledges that the Policy was designed to exceed express minimum regulatory requirements. However, it is Hydro One's view that in the context of a critical infrastructure environment more than minimum standards are necessary to provide protection. Hydro One also points out that their license also requires them to take all reasonable precautions to protect third-party information in its possession.

[88] Hydro One indicates that there are approximately 11 PWU members who are employed within Hydro One's core finance operations. However, other employees within the Accounting and Internal Control Clerk and Provincial Services roles regularly engage in project workflows, which are fluid and routinely are granted greater access to computer systems and SAP.

[89] In their August 5, 2025 submission, Hydro One addressed NERC's asset impact rating categories BES impact ratings. Hydro One has three High Impact Facilities containing BES cyber systems:

- The Integrated System Operating Centre (ISOC)
- The Ontario Grid Control Centre (OGCC); and
- Richview TS data Centre

[90] Hydro One identified the following 10 classifications that have regular access to the high impact assets for the purpose of maintenance and stations services activities as well as commissioning activities:

- P&C Technologist – maintenance and commissioning activities
- P&C Trainees – maintenance and commissioning activities
- P&C Engineer / Field New Grad – maintenance and commissioning activities
- P&C Engineer / Officer Supervisor– maintenance and commissioning activities
- SR P&C Supervisor – maintenance and commissioning activities
- UTS 3 – maintenance and commissioning activities
- UTS 2– maintenance and commissioning activities
- RME – maintenance and commissioning activities
- RME Apprentices – maintenance and commissioning activities
- Mechanical Maintenance - maintenance and commissioning activities.

[91] Hydro One indicates in their submission that the majority of their physical BES assets are rated as Medium Impact. These same classifications have regular access to Medium Impact assets. Hydro One identifies a number of classifications that are regularly employed at Hydro One's Transmission Stations and Sub-Stations. Hydro One advises that in addition to site access, the employees in these classifications routinely work with and/or design the core technical data and schematics that comprise Ontario's electricity grid.

[92] Hydro One insists that they need a common standard for screening all these individuals who have access to physical sites. They also point out that these facilities become command centres during storm responses and as such employees who are provided access during those events also need to be screened.

[93] The PWU submits that it is an exaggeration to suggest that because PWU members may perform perimeter inspections once or twice a year that would mean that they should be screened at the highest level. The PWU also notes that the NERC Standard only applies to "all physical access to its BES Cyber systems"

whereas Hydro One's Policy is applied to those with SAP access. SAP access and access to BES Cyber systems are not the same thing.

[94] The Hydro One assets listed as "Low Impact is an inclusive category, which applies as a regulatory default. Hydro One claims that the distinction between "Medium Impact" and Low Impact" is largely irrelevant as employees may be called to work at different assets at any given time.

[95] The PWU submits that the NERC Standard only applies to those employees who have "authorized cyber or authorized unescorted physical access to Critical Cyber Assets." The PWU notes the following with respect to the various levels of screening:

> Employees screened at Level 1 and Level 2 have either no access or non-critical access to SAP. Employees screened at level 2 include classifications such as Stockkeeper, Provincial Services Clerk, Lines Customer Support Clerk, Labourer, Truck Driver, and Regional Maintainer-Forestry. They assert it is unclear how these employees have any access to Hydro One's critical cyber assets. The PWU takes the position that these employees should not be subject to any screening.
>
> Employees screened at Level 3 contains 69% of PWU members, including those employed as Instructor, Job Clerk, Regional Maintainer-Lines, Stockkeeper, Helicopter Pilot. The PWU assert that Hydro One has not demonstrated that these employees have access to critical cyber assets, and whether that access includes "sensitive electronic access" as required for Level 3 screenings under the Policy.

[96] The PWU submits that the problem with the Policy is that Hydro One starts with the NERC Standard which is restricted to those employees with unescorted physical or cyber access to the BES cyber systems (which would be a very small percentage of the overall PWU represented workforce). Hydro One then seeks to expand the NERC Standard to employees who may have access to customer confidential information (i.e. credit card data) or who may have access to other employee financial information (i.e. expense reports) and relies on a couple of incidents from the past (i.e. the ISIS connected Co-op student) to expand both

the nature, level and intrusiveness of the searches conducted and to require those increased intrusive searches to a wider swath of employees. According to the PWU this is evident in the sheer number of PWU employees subject to Level 3 searches. There are a huge number of Regional Maintenance Lines ("RMLs") and other classifications who have no access to physical or cyber access to the BES cyber systems that are at Levels 2 and 3.

Driver's abstracts and credit checks

[97] Hydro One is of the view that drivers' abstracts and credit checks are a best practice and commensurate with the associated employees' physical and electronic access to Hydro Ones' sites and systems.

[98] Hydro One indicates that requiring driver's abstracts for employees who are not required to drive a Hydro One vehicle serves multiple purposes, including identifying a pattern or propensity to engage in adverse or illegal behaviour that risks Hydro One's assets and security, and identifying indifference to other's safety.

[99] Hydro One points out that a driving offense does not preclude an individual from employment with them. A final reliability decision resides with the Chief of Security Officer. An individual will not be deemed "Not Reliable" until after an interview is conducted. Hydro One uses such interviews to gauge the individual's attitude and sentiment towards the incidents and measuring the individual's propensity to engage in similar or other adverse behaviour in the future.

[100] The PWU does not take issue with driver's abstracts being required for those who drive a Hydro One vehicle. They accept that there is a reasonable relationship between having such private information and safely operating a Hydro One vehicle. PWU takes issue with requiring driver's abstracts for employees who do not drive a Hydro One vehicle. They are of the view that requiring driver's

abstracts from employees who do not drive a Hydro one vehicle is an invasion of their privacy without proper cause.

[101] Hydro One acknowledges that credit checks can be met with resistance because the information is "generally perceived to be more sensitive." However, according to Hydro One the data within the credit check corroborates other screening data, such as addresses, employment history, and map an employee's financial history relative to their peers by highlighting anomalous transactions or cash flows that might signal misrepresentation and trigger other screening tools. Hydro One asserts that credit checks are also necessary in light of the heightened security risks associated with Canada's critical infrastructure organizations.

[102] Hydro One points out that Stations Support Clerks and Job Clerks have access to sensitive electronic records and information, including customers' personal information, credit card, bank details and SIN information. Hydro One also points out that these employees format and update data on SAP.

[103] Hydro One points to areas identified by Public Safety Canada's Critical Infrastructure Directorate in a 2019 document titled *Enhancing Canada's Critical Infrastructure Resilience to Insider Risk*, which identifies 8 recommended security actions, including recommending pre-employment screening and the following with regard to ongoing employee security screening:

> Implement Ongoing Employee Security Screening
>
> Organizations should review and update their security screening of employees at periodic intervals (e.g. every 5 years) or as the situation warrants. It should be recognized that risk levels can change over time and consequently periodic background checks and credit checks comparative to the security level of any given position can identify unusual activities and behaviours that might have otherwise gone unnoticed. For instance, if an employee is taking on new responsibilities, or is moving to a position with a higher risk profile, a more thorough background check might be required.

[104] Hydro One notes that credit reports are recommended by the Directorate to identify individuals who may be likely to be influenced and/or compromised by malicious, state or non-state actors.

[105] The PWU points out that security action #1 recommends that employee access align with position risk levels; screenings “should be commensurate with the level of risk assessed to complete functions and tasks expected of that employee. Security action #6 suggests that employers should restrict access internally to mitigate insider risk.

[106] The PWU argues that Hydro One has done just the opposite, granting employee access to sensitive electronic files without necessity. The PWU asserts that many employees in Stockkeeper and Regional Maintainer-Lines, and Planning Scheduling Technician have critical SAP access that are not necessary for them to perform their duties.

[107] It must be noted that the Directorate recommendations do not constitute a legal obligation on the part of Hydro One to conduct such checks. They are merely recommendations. In addition, the recommendations do not include screening every employee. The recommendations focus on screening employees “based on the roles and responsibilities of their position.” In other words, the screening is to be targeted and based on risk, not applied to every employee of the organization.

[108] The PWU does not challenge ongoing screening of certain individuals who fall within the NERC Standard. The PWU’s position is that not every Hydro One employee presents a risk requiring screening or a driver’s abstract and credit check. In the PWU’s view, Hydro One has not explained or provided cause as to why existing employees who do not meet the NERC Standard need to be screened and provide credit checks or a driver’s abstract. These employees have a track record with Hydro One. Hydro One would have had the opportunity to check their refences when they were hired. Hydro One would have their address, SIN and other personal information on file. According to the PWU, ongoing employee

screening ought to be reserved for persons whose roles change and fall within the NERC requirements or provide some reasonable cause for concern.

[109] The PWU proposes that the levels of screenings reflect the NERC Standards and suggest the following changes to the screening process for PWU members:

Level 1 – Employees not subject to the NERC standards

- Identity verification
- Address verification (every seven years)

Level 2 – Employees subject to the NERC Standards

- Level 1 reliability screening as above
- Criminal records check

For employees at all screening levels, the following additional checks may be conducted as reasonably appropriate based on job duties:

- Driver's abstract (record and license verification) – for those employees required to drive Hydro One vehicles as part of their essential duties of their job.

- Reliability Interview – to address adverse information or to obtain more detail that may be required for a proper determination of reliability. The scope and content of these interviews must be subject to the PWU's approval and include PWU representation.

Evidence relating to other Canadian Electrical Sector Utilities/Companies

[110] Hydro One asserts that reliability screening is "normative" in the industry. Hydro One provided information about Hydro Québec's screening program, which they say applies to existing employees every 5 years and contractors every 3 years and is described as follows:

- Level 1 – Criminal background check, identity verification, employment/education verification
- Level 2 - Criminal background check, identity verification, employment/education verification, credit check, driver's abstract, media search

- Level 3 - Criminal background check, identity verification, employment/education verification, credit check, driver's abstract, media search and law enforcement records search.
- Level 4 - Criminal background check, identity verification, employment/education verification, credit check, driver's abstract, media search and law enforcement records search and in-person interviews inclusive of family/friends/neighbours.

[111] Unfortunately, the information provided by Hydro One does not include identification of which employees are subject to the various levels of screenings. There is no information as to whether the union at Hydro Québec agreed to such measures or whether they are found in a policy or procedure.

[112] The PWU notes that Manitoba Hydro has a less stringent policy. Manitoba Hydro's screening process consists of an identity verification and a criminal records check for new and existing employees, but it is unclear whether it applies to employees not covered by the NERC Standard. The PWU asserts that both Hydro Québec and Manitoba Hydro have fewer invasive processes.

[113] Hydro One also provided a Canadian Broadcasting Corporation (CBC) report of a Hydro Québec employee who was accused of spying for China and charged under the *Security of Information Act* and the *Criminal Code of Canada* ("*CCC"*) on November 14, 2022. The charges involved the fraudulent use of a computer, fraudulently obtaining a trade secret and breach of trust. The employee was a researcher who worked on battery materials with the utility's Centre of Excellence in Transportations Electrification and Energy Storage (CETEES). The CETEES develops technology for electric vehicles and energy-storage systems.

[114] The PWU points out that the Hydro Québec incident appears to involve the misappropriation of intellectual property and unconnected to an actual threat to critical infrastructure. They argue that it is unclear how any security clearance process would have led to a different result.

[115] Hydro One submitted a Statement by the Privacy Commissioner of Canada regarding a data breach at Nova Scotia Power along with media reports. The data breach appears to have affected 280,000 individual customers. The news reports reference that a “hack” occurred on March 19 but was only discovered on April 25, 2025. the utility did not pay any money to “hackers” in response to a ransom demand. Nova Scotia Power provided those affected individuals with a two year subscription to a credit monitoring service to reduce the potential for fraud. The news report also identifies a Nova Scotia Power customer who had her bank account drained. The news report does not identify whether any Nova Scotia Power employees were involved in the hack. The best one can make of this information is that the incident was one involving an external actor not an employee of Nova Scotia Power.

[116] Hydro One included in their submissions a news article dated February 20, 2024, about an OPG employee who had been charged under the *Security of Information Act* for allegedly sharing “safeguarded information.” A publication ban was imposed on the case.

[117] The PWU provided evidence relating to screening at OPG, where they represent the majority of unionized employees. The PWU points out that OPG is subject to NERC, and they are also subject to heightened obligations under the Canadian Nuclear Safety Commission (CNSC), which has regulations applicable to secure nuclear facilities like those operated by OPG in Pickering and Darlington, Ontario. Despite being more tightly regulated, the PWU asserts that OPG has a less intrusive security screening policy.

[118] The PWU provided a publicly available document from OPG titled *Security Clearance*, which outlines the screening OPG follows for granting security clearances. The PWU submits that despite the heightened regulations and concerns related to nuclear facilities, OPG’s security clearance policy does not mandate credit checks as a standard requirement. In addition, Driver’s abstracts are not mandated for all employees either.

[119] Hydro One submits that the OPG policy is irrelevant as it arises in a different context under different regulations. Hydro One points out that OPG employs armed guards and other security protocols at its facilities. Hydro One in the alternative argues that the OPG policy supports their position in that the OPG policy exceeds CNSC requirements by screening all employees and requiring certain employees to provide drivers abstracts and credit checks at a manager's discretion. Hydro One also points out that OPG has three levels of screening and they use the Treasury Board Secretariat (TBS) Personal History Questionnaire (PHQ) for level II candidates.

[120] Hydro One acknowledges that their reliability screening program is generally regarded as the "most robust reliability screening program…"

The 2020 Canadian Centre for Cyber Security (CCCS) Bulletin and 2022 Canadian Security Intelligence Service (CSIS) Report

[121] Hydro One points to a cyber threat bulletin issued by the Canadian Centre for Cyber Security (CCCS) in 2020, which notes that state sponsored cyber threat actors have been targeting parts of the Canadian electricity sector since at least 2012.

[122] I note that this report indicates that the cyber threat activity against Canada's electricity sector has consisted mostly of fraud and ransomware attacks by cyber criminals, as well as espionage and pre-positioning by state-sponsored actors. They judge that it is very unlikely that state-sponsored cyber threat actors will intentionally seek to disrupt the Canadian electricity sector and cause major damage or loss of life in the absence of international hostilities. However, there is a concern associated with the connections between the US and Canadian grids. There is nothing in this bulletin suggesting that electricity transmission and distribution companies ought to screen all their existing employees.

[123] Hydro One also relies upon a 2022 Canadian Security Intelligence Service (CSIS) Report, which raises concerns about foreign states seeking to acquire access or control over critical infrastructure such as Hydro One's network, to advance their own military and intelligence capabilities, as well as adversely affect the Canadian economy.

[124] This report certainly raises many concerns about potential threats to critical infrastructure, but mostly from external actors not current employees. There is nothing in this report that suggests that electricity transmission and distribution companies ought to screen all their existing employees.

The OEB White Paper

[125] Hydro One also included in their submissions a June 1, 2017 OEB White Paper titled *Cyber Security Framework to Protect Access to Electronic Operating Devices and Business information Systems within Ontario's Non-Bulk Power Assets* (the "White Paper'). The OEB regulates transmitters and distributors (also referred to as Local Distribution Companies or "LDCs") who operate Ontario transmission and electricity distribution networks of which Hydro One is the largest.

[126] The White Paper is an OEB initiated cyber security consultation to develop a policy and reporting requirements to provide a measurable assurance from Ontario's natural gas and electricity entities that they are taking appropriate action with respect to their security, reliability and privacy obligations. The White Paper discusses its "Risk Profile Tool" which allows LDCs to be categorized objectively as either high, medium or low and have defined security controls for each level. The White Paper includes no recommendations relating to reliability screening of employees.

[127] A White Paper is a policy document; it may present policy preferences before legislation is introduced. But a White Paper is not legislation, regulation or an enforceable policy under any legislation. This White Paper was written 8 years

ago and no legislation, regulation or policy has been introduced requiring Hydro One to conduct reliability screening on existing employees.

[128] I have not been provided with any government legislation, regulation, policy or direction requiring Hydro One to undertake security screening of existing employees, save and except the NERC Standard.

Decision

[129] Hydro One initially argued that the grievance was untimely and ought to be dismissed. Hydro One did not advance this argument at the hearing. But even if they did, the grievance would not be dismissed as untimely.

[130] The issue in dispute between the parties is of an ongoing nature, the ongoing application of the Policy to PWU members. The PWU has maintained their position that the Policy is overbroad since the Policy was brought to their attention. The PWU has engaged in a dialogue with Hydro One in an attempt to resolve the grievance. Hydro One has provided additional information to the PWU to try and convince them that the Policy is reasonable. Both parties have made good faith efforts to resolve their differences. Unfortunately, the parties are now at an impasse and I must resolve the dispute.

[131] Hydro One has not been prejudiced in any way by the delay in having this matter heard. In these circumstances, if necessary, I would extend the time limits as I am permitted to do, both under Article 3 of the Collective Agreement and s. 48(16) of the *Labour Relations Act, 1995* S.O. 1995, c.1 Sched A.

[132] I now turn to the merits of the grievance.

[133] There is no explicit language in the Collective Agreement addressing security clearances or reliability screening. The only agreement between the parties is the 2023 Side Letter, which is explicitly outside the Collective Agreement

and was recently renewed. The 2023 Side Letter is subject to these proceedings. Accordingly, the real issue in dispute requiring resolution is whether or not the Policy is a reasonable exercise of management rights.

[134] As indicated earlier, the PWU does not challenge the application of the policy for those who seek to be hired by Hydro One. This is not too surprising as such individuals are not represented by the PWU until after they are hired into employment.

[135] The PWU also does not challenge the application of the NERC Standard. The PWU accepts Hydro One's legal obligation to have a PRA program for certain employees who have authorized electronic access and/or authorized unescorted access to its BES Cyber Systems. The PWU challenges the broader application of the Policy, taking issue with what they assert are inappropriate screening levels applied to their members and unreasonable screenings (criminal records, credit checks and drivers abstracts for non-driving employees, and reliability interviews).

[136] Hydro One insists they need to address concerns beyond the NERC Standard, and the Policy is an important component of their overall risk management program.

[137] Hydro One asserts that existing employees are not presumptively lower risk than new hires. Hydro One points out that the vast majority of their employees were hired prior to reliability screening being introduced and therefore no presumption can be made as to the threat they pose to Hydro One.

[138] There can be no doubt that Hydro One, as a utility that is part of Canada's critical infrastructure, has the right to protect their assets. Screening potential applicants is a reasonable way of ensuring that new employees, who are not known to Hydro One, are suitable and reliable. As noted in the *Police Records Check Reform Act, 2015*, S.O. 2015, c. 30, search of the Canadian Police Information Centre (CPIC) data base is an appropriate screening tool in

determinations of employment suitability. There is recognition that as a person unknown, employers ought to have tools to assist in determining the suitability or reliability of candidates for employment.

[139] Hydro One has developed a robust screening process for new hire candidates and they should be applauded for their due diligence. However, with respect, different considerations apply to persons who are already employed with Hydro One and have an established relationship and record.

[140] In *Ottawa (City) v. Ottawa Professional Fire Fighters Assn.,* (2007) 169 L.A.C. (4th) 84 (M. Picher), upheld [2009] O.J. No. 2914 (Div. Crt.) ("*City of Ottawa")*, Arbitrator Michel Picher notes the very important distinction between pre-employment screening and screening of existing, employees, where he states as follows:

> The person who presents himself or herself at the door of a business or other institution to be hired does so as a stranger. At that point the employer knows little or nothing about the person who is no more than a job applicant. In my view, the same cannot be said of an individual who has, for a significant period of time, been an employee under the supervision of management. The employment relationship presupposes a degree of ongoing, and arguably increasing, familiarity with the qualities and personality of the individual employee. The employer, through its managers and supervisors, is not without reasonable means to make an ongoing assessment of the fitness of the individual for continued employment, including such factors as his or her moral rectitude, to the extent that it can be determined from job performance, relationships with supervisors and other employees, and such other information as may incidentally come to the attention of the employer through the normal social exchanges that are common to most workplaces. On the whole, therefore, the extraordinary waiver of privacy which may be justified when a stranger is hired is substantially less compelling as applied to an employee with many months, or indeed many years, of service.

[141] I agree with Arbitrator Picher, and I believe that there is another distinction that can be made between individuals seeking employment and those who are already gainfully employed by an employer. The distinction is based on choice and more precisely the choice to give consent to release private information.

[142] A prospective employee objecting to providing a criminal background check can walk away and they have lost nothing other than the prospect of being employed by Hydro One. They are able to choose to protect their privacy and seek employment elsewhere. However, an employee who is already gainfully employed by Hydro One is in a much more precarious position. The employee who is already employed, faces a Hobson's choice between giving up their privacy or being disciplined or worse losing their livelihood. Some might say they face a Catch-22.

[143] An existing employee at Hydro One has an established track record and the protections of the Collective Agreement that must be respected.

[144] Hydro One points out that changes can occur in one's life that may make the person more vulnerable to being recruited by a foreign state or make them less reliable. That may be true of any individual, but does that possibility justify a requirement that all existing employees must arbitrarily provide private information to Hydro One?

[145] The focus in this matter concerns the interpretation of management rights and employee rights found in the Collective Agreement between Hydro One and the PWU. In particular, the focus of the analysis is on Hydro One's managerial rights provided for under the Collective Agreement, to unilaterally introduce a rule or policy that all employees be subject to Reliability Screening. Article 7 addresses the managerial rights of Hydro One and it provides:

> The Company has and shall retain the exclusive right and power to manage its business and direct its working forces including, but without restricting the generality of the foregoing, the right to hire, suspend, discharge, promote, demote and discipline any employee. The Company shall exercise the said functions in accordance with the provisions of this Collective Agreement.

[146] On the other side of the ledger are rights of employees found in the various provisions of the Collective Agreement, which curtail Hydro One's managerial

rights. Most relevant to this matter is Article 2 (Grievance Procedure) generally and in particular 2.1, which provides as follows:

> Any allegation that an employee has been subjected to unfair treatment or any dispute arising from the content of this Agreement shall be understood to be a fit matter for the following grievance procedure. All matters of grievance by an employee nor group or class of employees whom the Union is the bargaining agent and which the Union may desire to present shall be dealt with in accordance with the following procedure.

[147] Article 2.5 addresses disciplinary matters and the imposition of discipline on employees.

[148] Article 2A also addresses discipline and discharge. Most relevant to this matter is 2A.1, which provides

> Any allegation that an employee has been demoted, suspended, discharged or otherwise disciplined without just cause shall be a fit matter for the grievance and arbitration procedures as provided for in this Collective Agreement.

[149] The right to grieve under this Collective Agreement is broad and includes unfair or unjust treatment. Employees enjoy various protections prior to discipline being imposed, including the right to notice and a Disciplinary Interview, and the right to union representation.

[150] Article 3 provides an expedited and robust arbitration process, which includes the power to provide interim relief.

[151] The PWU also relies upon Article 4, which addresses changes to working conditions during the term of the Collective Agreement, the relevant provisions provide as follows:

> **4.1** Working conditions during the term of this Agreement shall be as outlined in this Agreement and Mid-Term Agreement [1] except such Mid-Term Agreements as are agreed obsolete by the parties.
>
> In addition, the general environmental privileges surrounding an employee shall also be considered as working conditions. These privileges would include such things as wash-up time, transportation facilities, safety appliances, general safety or health precautions.
>
> **4.2** Any modification within the confines of this Agreement shall be subject to agreement by the Company and the Union's executive…

[152] While the Policy does not refer to an employee's right to challenge a finding through the grievance and arbitration procedure, the Policy cannot defeat a right found in the Collective Agreement or a statutory right. The Collective Agreement provides PWU members with the right to union representation and the right to file a grievance and proceed to arbitration. The right to arbitration is enshrined in *s. 48 of the Labour Relations Act, 1995.* To the extent that there might be any doubt, I find that a PWU member has the right to union representation prior to any disciplinary action being taken and the right to file a grievance and proceed to arbitration challenging any decisions made under the Policy that may be characterized as unfair or unjust, see *Ontario Hydro and Ontario Hydro Employees Union, Local 1000 et al*. (1983) 41 OR (2d) 669 (CA).

[153] Turning to management rights, there is no dispute that the general principles applied when examining unilateral employer policies that may have disciplinary consequences is well entrenched in the arbitral jurisprudence and has its genesis in the award of *Re Lumber & Sawmill Workers' Union, Local 2537, and KVP Co.* (1965), 16 L.A.C. 73 (Robinson) ("*KVP"*). The framework for reviewing a unilaterally imposed employer rule is set out in *KVP* as follows:

- It must not be inconsistent with the collective agreement.
- It must not be unreasonable.

[1] A Mid-Term Agreement is a modification of the Collective Agreement executed by the parties on the prescribed form (a specimen of which is shown below) during the term of the Collective Agreement.

- It must be clear and unequivocal.
- It must be brought to the attention of employees affected before the company can act on it.
- The employee concerned must have been notified that a breach of such rule could result in his discharge if the rule is used as a foundation for discharge.
- Such rule should have been consistently enforced by the company from the time it was introduced.

[154] The *KVP* test has been judicially endorsed by both the Ontario Court of Appeal, *Metropolitan Toronto (Municipality) v. C.U.P.E.* (1990), 74 O.R. (2d) 239 (C.A.) and the Supreme Court of Canada in *Communications, Energy and Paperworkers Union of Canada, Local 30 v. Irving Pulp and Paper, Ltd.* [2013] 2 S.C.R. 458 (*"Irving Pulp and Paper*").

[155] When an employer's unilateral rule or policy has disciplinary consequences, it is well accepted that such a unilateral rule or policy must be reasonable. This principle of reasonableness is anchored in the just cause provisions of a collective agreement, which imposes upon management an obligation to only impose discipline on employees for just and reasonable cause. An unreasonable rule or policy can never justify a disciplinary response.

[156] Arbitrators generally apply the KVP test using a "balancing of interests" approach to assess unilaterally imposed employer rules or policies affecting an employee's individual privacy rights.

[157] As noted by the Supreme Court of Canada in *Irving Pulp and Paper, supra,* in the earliest privacy cases using a balancing of interests approach, arbitrators generally found that employers could only exercise a unilateral management right to search an individual employee's personal effects if there was a reasonable suspicion that the employee had committed theft. Universal random searches – that is, random searches of the entire workforce-were rejected as unreasonable

unless there was a workplace problem with theft and the employer had exhausted less intrusive alternative measures for addressing the problem. This approach was later applied to random drug testing, even in safety sensitive environments, where arbitrators rejected unilaterally imposed universal random testing policies unless there had been a work place problem with substance abuse and the employer had exhausted alternative means for dealing with the problem.

[158] The matter at hand is analogous to personal searches and random drug testing policies. All these cases include management exercising their right to provide for a safe workplace and protect their assets. They all also include recognizing employees' individual rights to protect their privacy. In my view, it is appropriate to apply the same test and balancing of interests in the matter before me as I did in *Rouge Valley Health System v. ONA,* 2015 CanLII 24422 (ONLA).

[159] The interests at play in this matter are very important to both parties and to society as a whole. The PWU emphasizes the importance of their members' individual privacy rights. While Hydro One argues that their right to provide a safe and healthy workplace, protect their assets and insure the protection of the provincial electrical system requires a robust reliability screening procedure.

[160] It has been long recognized in the arbitral jurisprudence that as a general rule an employee's life outside the workplace is their own business and what they do outside the workplace is of no concern to their employer, unless the employee's conduct detrimentally affects the employer's reputation, renders the employee unable to properly discharge their employment obligations, causes other employees to refuse or be reluctant to work with that person, or inhibits the employer's ability to efficiently manage and direct their operations. Arbitrators have long recognized that unless a substantial and legitimate business reason exists, the employer has no authority, control, interest or jurisdiction over an employee's behaviour outside the workplace.

[161] However, it is also well settled that off-duty conduct of an employee which is found to be detrimental to the employer does constitute grounds for discipline, see *Re Millhaven Fibres Ltd and Oil, Chemical and Atomic Workers Loc. 9-670* (1967), 1 (A) Union-Management Arbitration Cases, 328 (Anderson) and *Re Domtar Forest Products and IWA Canada Lo. 2693* (1990), 14 LAC (4th) 188 (Aggarwal).

[162] I agree with the PWU that the individual rights of employees at issue in this matter are significant. An individual's right to privacy, including the right to protecting their personal financial information is recognized in the common law, see *Jones v. Tsige* (2012), 108 O.R. (3d) 241 (C.A.), and in legislation such as *PIPEDA*. The information found in a credit report check is sensitive financial information that employees are not normally required to disclose to their employer.

[163] In *Spectra Energy v. Canadian Pipe Line Employee's Association*, (2011), 211 LAC (4th) 130 (Liang), it was found that compelling production of an employee's driving abstract infringes upon their privacy rights. Arbitrator Liang found that in the absence of evidence of an existing problem that requires action be taken by the employer, the requirement to provide a driver's abstract was overly broad and unreasonable.

[164] In the matter at hand the PWU concedes that those who drive a Hydro One vehicle as part of their essential duties can reasonably be required to provide a driver's abstract. The PWU only objects to production of driver's abstracts by those who do not drive a Hydro One vehicle in the course of their normal duties.

[165] The information being sought by Hydro One includes information that requires an employee's consent to obtain. As such, the employee clearly has a direct interest and reasonable expectation of privacy over such information.

[166] I agree that an individual employee's rights, including the right to privacy are important rights that are protected at common law and protected from state

intrusion pursuant to the Canadian *Charter of Rights and Freedoms* (the "*Charter*"). The right to privacy is a fundamental legal right that should not be easily abrogated or constrained by employers. This is particularly so in the absence of just and reasonable cause.

[167] However, these individual rights are not absolute and there are circumstances where the rights of the collective outweigh the rights of the individual. While an individual employee's right to privacy is fundamental, so too is the right of all employees to have a safe and healthy workplace.

[168] A nuanced contextual approach must be adopted when applying the *KVP* test, and the balancing of interests. Context is extremely important when assessing the reasonableness of any workplace rule or policy that may infringe upon an individual employee's rights. The authorities reveal a consensus that in certain situations, where the risk to health and safety is greater, an employer may encroach upon individual employee rights with a carefully tailored rule or policy. But the authorities also reject as unreasonable random or universal intrusion into employee's privacy rights unless there is a workplace problem and less intrusive means have been exhausted.

[169] Hydro One argues that they have been directed to consider implementing requirements that extend beyond the minimum NERC Standard. Hydro One submits that the Policy is designed to address a number of staff risks, which are summarized in their submissions as the following four relevancy nexus criteria:

- Safety of the Grid or others
- *Code of Conduct* expectations
- Role specific concerns
- Brand and reputation concerns

[170] Hydro One points out that reliability screening is a "normative" practice in other organizations such as in the Government and financial services sectors that

engage in employee rescreening and use the “same family of tools for the rescreening of employees…” This may well be true with respect to new employees. However, I have not been provided with any policy that is as broad as Hydro One’s Policy. By their own admission, Hydro One has selected “the most robust” policy when compared to other hydro utilities, such as Hydro Québec and Nova Scotia Power who have actually had security incidents.

[171] Hydro One has provided a great deal of evidence about the potential risks and concerns they and Federal government agencies (e.g. CSIS) have with regard to not only critical infrastructure but also general concerns that apply to other employers who provide services to the public. However, the only legislation or regulation that has been imposed by government is the NERC Standard.

[172] There can be no doubt that Hydro One’s business is highly safety sensitive and is part of Canada’s critical infrastructure, but the issue remains, do the general potential threats identified by Hydro One provide reasonable cause or justification for the intrusive screening of all existing employees? I think not.

[173] In my view, the overwhelming arbitral jurisprudence, that has been endorsed by the Supreme Court of Canada, supports the view that subjecting existing employees to security screenings involving a requirement to provide consent to disclose private information is unreasonable, unless there is a workplace problem that exists and other less intrusive alternatives have been exhausted.

[174] Hydro One has not demonstrated a general problem with respect to security. Hydro One has provided the following examples:

- Co-op student who became an ISIS recruiter. There is no evidence that this employee was a PWU member or that he did anything dishonest while employed by Hydro One.
- A Chinese National who was rejected for a position at Hydro One, assisted in identifying two long service Hydro One employees who might be

unreliable. I have no information as to whether these employees were PWU members or whether any misdeeds on their part were identified.

- 2020 PRA clearance case that was not identified as a PWU member nor was any wrong doing identified.
- 23 year old Co-op student committing mortgage fraud was not an existing Hydro One employee.

[175] Mr. Chester's evidence relating to the long-standing Hydro One employee who was subject to a PRA and admitted to being convicted of murder seems to support the PWU's position that existing employees have a track record to prove their reliability and the additional screening is an unwarranted invasion of existing employee's privacy. The employee admitted to their past criminality and despite the horrible crime they committed, they had an established record that demonstrated their rehabilitation.

[176] The evidence simply does not reflect a general problem in this workplace that would justify arbitrarily invading the privacy of all employees. Much of the evidence presented to me is speculative and based on concerns that have generally been raised in the media and by government agencies. None of the examples provided were identified as existing employees represented by the PWU. Where Hydro One has identified potential threats, they have not identified any existing PWU represented employee who committed any breach of trust or security. The vast majority of threats that have been identified in the material provided by Hydro One are external threats, or threats by candidates/new hires and not existing employees who present the threat.

[177] The Policy equates access to SAP, a system utilized by many large companies, with the critical systems covered by the NERC Standard. SAP is not integrated with the critical systems covered by the NERC Standard. The SAP system is separate and while I accept that the information contained in SAP is sensitive, there is no evidence of any misuse of the SAP system by any existing PWU represented employee. Furthermore, I am not satisfied that Hydro One cannot configure SAP to restrict access for certain employees to certain

information. In my view, Hydro One has an obligation to demonstrate that such restriction is unmanageable or not feasible before they can invade employee's privacy rights.

[178] Hydro One has created a Policy that applies equally to both new employees and current employees, by assuming that anyone who has not previously been subjected to a security screening is as much a threat as someone who is unknown to Hydro One. With all due respect, I find this io be absurd as it fails to take into consideration the fact that existing employees are known to Hydro One and have an established track record.

[179] The Policy is not tailored towards the NERC Standard, but rather it is tailored towards any and all potential threats that Hydro One's security department and contractors wish to mitigate, including threats that all employers face such as inappropriate conduct and harassment. While the purpose is understandable from a risk assessment point of view, the Policy itself goes well beyond what one would find to be reasonable when applied to existing employees given the lack of any evidence to demonstrate a real threat or general problem from such employees that could not be mitigated by using less intrusive methods.

[180] The Desjardins case is an example where security clearances were found to be reasonable, but the other less intrusive measures were found to be lacking. In my view, the Desjardins case represents an example where intrusive security measures failed, and the real problem was addressing the less personally intrusive means of providing protection.

[181] Hydro One has focused on employee security screening and failed to provide evidence that they cannot address these speculative threats and concerns by enhancing the following areas noted by the OPC in Desjardins:

- Access controls and data segregation
- Oversight and monitoring

[182] As noted by the OPC, methods of protection should include organizational and technological measures to protect personal information. Hydro One has not demonstrated to me that they could not limit access and permissions for employees to only have information necessary for performing their duties.

[183] The OPC also noted that oversight and monitoring are indispensable to any personal information protection system. Hydro One has not demonstrated that additional oversight and monitoring will not provide a reasonable amount of protection of their information and other systems, including SAP.

[184] I agree with the PWU that requiring employees who do not drive a Hydro One vehicle to consent to disclosing their driver's abstracts is overly invasive for those existing employees who do not fall within the NERC Standard. Hydro One indicates that the driver's abstract assists in assessing an employee's propensity to engage in safe behaviours consistent with their *Code of Business Conduct* and safety culture. I fail to see how this information is needed for those employees who do not operate a Hydro One vehicle as part of their regular duties and have an established record with Hydro One.

[185] The personal financial information found in a credit report is inherently sensitive and employees clearly have an interest and reasonable expectation that such information will remain private. I agree with the PWU that requiring existing employees to consent to a credit check is unreasonable unless a real threat can be identified.

[186] Hydro One indicates that a credit check helps validate information provided by the employee. But Hydro One already has significant information on file for existing employees, including their SIN, earnings from Hydro One and address for sending them tax documents. Information can be confirmed by requiring that employees provide a copy of their driver's license or passport, which are government issued documents. Hydro One has not provided any evidence of any existing employee providing a false address or other information. While one

can see how Hydro One might want to verify information from a new employee, the same cannot be said for an existing employee in my view.

[187] The requirement of all employees to submit to a criminal records check is also unreasonable in the absence of a legislative, regulatory requirement or a real and demonstrable problem is generally unreasonable, see *Ottawa (City) and Ottawa Professional Firefighters Association, supra*. I can appreciate how those who meet the NERC Standard have access to critical infrastructure and renewed periodic screening is reasonable to protect those assets that are essential to the public. I have difficulty accepting that Hydro One needs to obtain criminal records checks for all employees simply because they may be granted access to other sensitive systems or locations. In the absence of any reasonable concern about an individual employee, requiring a criminal records check of an existing employee who is not subject to the NERC Standard is unreasonable.

[188] One example is a General Helper, who would be screened at Level 1 and required to provide a driver's abstract and have a criminal records check. I fail to see how a General Helper is any real threat to any sensitive systems at Hydro One.

[189] Another example is a Labourer, who is screened at Level 2 and would also have the same types of screening as a General Helper, but also have education and reference checks. Labourers are not hired for their education and in any event such employees would have been subject to reference checks when they were hired. I also fail to see how a Labourer would be a threat to Hydro One's sensitive systems.

[190] Hydro One has grouped the vast majority of employees into Level 3, the highest level, which includes the employees covered by the NERC Standard. I have a problem with casting such a wide net and I fail to see how those employees who do not have authorized cyber or authorized unescorted physical access to

Critical Cyber Assets, are being treated the same as those covered by the NERC Standard.

[191] I acknowledge that Hydro One uses substations and other facilities as command centres for storm response. However, staff are not unescorted when they meet and deploy at such locations. I have been provided with no evidence that employees who respond to storms present a problem to safety and security at Hydro One. These employees are tasked with the job of repairing assets, I have not been provided with any evidence of any such employee committing sabotage or committing any other mischief that might affect the distribution and transmission of electricity.

[192] I have also not been provided with any authority that upheld a policy as broad as the Hydro One Policy. The only cases referenced by the parties involving criminal records checks are the *Ottawa (City) and Ottawa Professional Firefighters Association, supra,* and my award in *Rouge Valley Health System, supra*. In both cases the policies were with respect to criminal records checks and they were found to be unreasonable in both instances.

[193] Hydro One points out that they have a statutory duty under the Ontario *Human Rights Code* (the "*Code*") to provide a workplace free from harassment and discrimination.

[194] The statutory duty under the *Code* fall upon all employers and to this extent Hydro One is not in a unique situation. The statutory duties are couched in terms of requiring reasonable steps. This fits nicely into the *KVP* analysis, which is also based on reasonableness and balancing interests. I do not see how obligations under the *Code* would justify infringing upon existing employee's privacy rights unless there were a particular problem that needed to be addressed or Hydro One had reasonable cause to believe that an individual employee would pose a risk.

[195] Hydro One relies upon the statutory duty found in s. 25(2)(h) of the *Occupational Health and Safety Act* ("*OHSA*"), which provides that employers are required to "take every precaution reasonable in the circumstances for the protection of the worker."

[196] The *OHSA* requirement is also an obligation that falls upon all employers in Ontario. It is not a license to invade employee privacy rights without cause. The language is also couched in reasonableness and fits neatly within the KVP analysis, which is also based on reasonableness. There is nothing in the *OHSA* that requires security screenings in this or any other workplace, without a clearly identified problem.

[197] Hydro One also relies upon s. 217.1 of the *Criminal Code of Canada* requires employers to take reasonable steps to prevent bodily harm to any person arising from work performed in the workplace.

[198] Once again, this obligation is not unique to Hydro One, as it applies to all employers. The statutory obligation speaks to taking reasonable steps, which in my view applies to specific situations where there is a known threat in the workplace. If Hydro One knew of a particular employee who posed a threat, then they must take reasonable steps to address the threat. But the obligation does not in my opinion grant an employer license to violate all employee's right to privacy.

[199] Hydro One has the right to assess the risk that a new employee might pose to their operations, the public and their staff. I also accept that there may be situations where Hydro One may have reasonable and probable cause to make inquiries of an existing employee who may present a threat. However, screening every employee goes beyond the statutory duties under these statutes. Neither the *Code*, nor the *OHSA* nor the Criminal Code require employers to conduct reliability screening or grant a license to employers to violate an employee's privacy rights.

[200] Hydro One also relies on other common law tort duties such as negligent retention and vicarious liability. Once again the common law is couched in terms of reasonableness and must take into consideration *Charter* values, such as the right to privacy, see *Jones v. Tsige, supra*. I have been provided with no authority where employer negligence was found for not screening existing employees. As indicated earlier, employees enjoy a common law right to privacy, particularly of their financial information. I have been provided with no authority where a court or tribunal found it reasonable to require existing employees to be subject to security screenings such as those found in the Policy.

[201] Hydro One relies on an OLRB decision between *Bruce Power and CUSW* [2018] OLRD No. 811. This case is distinguishable based on the facts involving different collective agreement language and an employee who had been charged with offences under the *CCC*. The case involved revoking a security clearance at a nuclear facility, which is subject to government regulations. The decision did not involve a unilaterally implemented policy requiring the screening of all existing employees. The context is different and the decision is not helpful.

[202] Hydro One argues that the decision of the Ontario Court of Appeal in *Khorsand v. Toronto Police Services Board* 2024 ONCA 597, supports their position on management's right to conduct security screening. I disagree with this submission as once again the context and issues at play were different from the matter before me. The case before the Court of Appeal involved an individual who had applied for a job as a special constable with the Toronto Community Housing Corporation (TCHC). The Toronto Police Service (TPS) conducted the background check for the TCHC, which the individual failed. The individual then asked the TCHC and TPS to disclose reasons and information relied upon for making that decision. The TPS refused to provide any information beyond that which had been provided to the individual under the *Municipal Freedom of Information and Protection of Privacy Act*, RSO 1990, c. M. 56. The individual applied for judicial review of the TPS decision. A majority of the Divisional Court found that judicial

review was available. The Court of Appeal allowed the appeal finding that judicial review was not available because the issue is not of a sufficiently public character.

[203] The issue before the Court of Appeal was access to judicial review, and their comments about the legitimacy of security screening was *obiter* and in the context of pre-employment screening. As stated from the onset, the case before me is not pre-screening potential employees. This case involves a Policy that Hydro One wishes to apply equally to new hires and existing employees. The issue before me arises under the Collective Agreement between these parties and determining management's right to unilaterally implement such a Policy to screen existing employees.

[204] After carefully considering the parties' submissions, I find that the Policy is overly broad and unreasonable. The Policy does not distinguish between new hires and existing employees. The Policy is also overly broad going beyond what is required under the NERC Standard and applying the security screening to all employees. The requirement to have employees consent to provide a credit report check and driver's abstract search is unreasonable and an unnecessary invasion of privacy unless Hydro One has just cause to suspect that an individual employee may pose a real threat.

[205] In light of my findings, I do not believe it is necessary to make any specific comments with respect to the resolution of doubt interview at this time. PWU members have the right to file a grievance if they feel they have been treated unfairly and that may include being subject to a resolution of doubt interview. If the resolution of doubt interview has disciplinary consequences, then Hydro One must abide by the terms of the Collective Agreement.

[206] Finally, given my finding that the Policy is unreasonable and violates the Collective Agreement, it is not necessary to address the PWU's allegation that the Policy violates *PIPEDA*.

[207] Therefore for all the reasons stated above am allowing the grievance, and making the following orders, which are only applicable to PWU members (Regular and Hiring Hall):

- The Policy must be amended to limit its application to those employees subject the NERC Standards and for cause situations, save and except Hydro One may verify an employee's identity and address every seven years;

- Hydro One is to provide the PWU with a list of employees and their classifications that fall within the NERC Standard;

- The Policy must be amended to exclude the requirement to provide a credit check, unless Hydro One has reasonable cause to suspect that an individual employee may be a threat;

- The Policy must be amended to exclude driver's abstracts for those who do not drive a Hydro One vehicle as part of their normal duties, unless Hydro One has reasonable cause to suspect that an individual employee may be a threat;

- The Policy must be amended to provide for union representation in accordance with the Collective Agreement;

- The Policy must be amended to provide for the right to file a grievance and proceed to arbitration under the Collective Agreement.

[208] I remain seized to address any issue fairly raised by the grievance but not addressed in this award, including implementation of my orders.

Dated at Toronto, Ontario this 29th day of January 2026.

John Stout - Chief Arbitrator