Federal Court Cour fédérale

Date: 20250812

Docket: T-258-24

Citation: 2025 FC 1369

Ottawa, Ontario, August 12, 2025

PRESENT: The Honourable Madam Justice Saint-Fleur

BETWEEN:

KIMBERLY MUMA

Applicant

and

ATTORNEY GENERAL OF CANADA

Respondent

JUDGMENT AND REASONS

I. Overview

[1] This is an application for judicial review of a decision by the Acting Director of Public Services and Procurement Canada [PSPC]'s Industrial Personnel Security Services Directorate [Acting Director], dated January 12, 2024 [Decision].

[2] PSPC screens applicants for, and provides security designations to, a variety of individuals. These individuals include those working under contract with Government departments, such as the Applicant in this case. After completing a Review for Cause, PSPC revoked the Applicant's Reliability Status, administratively closing his ability to hold a Secret or Top-Secret security clearance.

[3] The former *Standard on Security Screening* [*Standard*], in place at all times material to this proceeding, outlines three levels of security screening: Reliability status, Secret clearance, and Top-Secret clearance. Reliability status is the minimum standard of security screening for positions requiring unsupervised access to Government of Canada protected information, assets, facilities or information technology systems. Individuals cannot hold a Secret or Top-Secret clearance without meeting the requirements for Reliability status. Thus, when the Applicant's Reliability status was revoked, his ability to hold Secret or Top-Secret clearance was "administratively closed."

[4] The Applicant brings this application for judicial review on the basis that the Decision was both procedurally unfair and unreasonable.

[5] For the reasons outlined below, I dismiss this application.

II. Background Facts

[6] The Applicant is a software engineer with over 35 years of experience in security contracting. At all material times, he was a contractor with the Department of National Defence

[DND], where he developed and tested software solutions to enhance IT network security for DND and the Canadian Armed Forces.

[7] The Applicant says he typically worked with multiple devices and computers in the course of his duties. Some were unclassified, and one was a classified workstation connected to the Defence Wide Area Network [DWAN] (an Intranet-type network internal to DND).

[8] On November 25, 2022, PSPC received information from DND about a November 15, 2022, cyber incident where the Applicant was found to have inserted a device containing a "credential stealing tool" into his classified DWAN workstation [the Incident].

A. *The Incident*

[9] The Applicant attests that the Incident was related to a security issue he was trying to address in mid-2022. To develop a solution to this issue, he says he used source code present on two portable file storage devices: 1) a "Trinkey Device" (i.e., a Raspberry Pi/Pico microcontroller, his own property) [Trinkey], and 2) a USB Flash Drive (provided to the Applicant by DND/Canadian Forces personnel, specifically for his work at DND) [Flash Drive].

[10] In September or October 2022, the Applicant affirms he was using his Trinkey on an unclassified computer to develop and test his proposed solution, and at one point mistakenly inserted it into the DWAN workstation rather than the Unclassified Computer. He unplugged the Trinkey less than five minutes later, and no security alert resulted.

[11] On November 15, 2022, the Applicant inserted the Flash Drive into the DWAN workstation (rather than the Unclassified Computer) to complete and submit his timesheet. Once his timesheet was submitted, about five minutes later, he unplugged the Flash Drive.

[12] The Flash Drive contained a program called "Mimikatz," a tool used to learn the C: programming language that is also capable of experimenting with Windows security and stealing credentials. The Applicant says he previously transferred the Mimikatz files onto the Flash Drive and forgot about them. There is no evidence on the record that the Flash Drive ran or initiated any program, including Mimikatz, on the DWAN workstation.

[13] The Applicant did not take any steps to report either incident when they occurred.

B. *The Investigation*

[14] Both DND and PSPC conducted investigations into the November 2022 Incident. DND conducted a forensic analysis of the Incident, while PSPC appraised the Applicant's overall trustworthiness as a Reliability Status and Top Secret clearance holder. As will be noted below, DND's investigation is not the subject of this judicial review.

[15] DND provided an infographic summary to PSPC, which identified the Incident's Operational Impact as "Medium" and alleged that the Applicant "confirmed deliberate use of an exploitation toolset on the DWAN and appears unrepentant." DND indicated that an IT review of the Incident was ongoing.

[16] A PSPC Senior Case Manager [Investigator] prepared a New Adverse Information Report [NAIR] in response to the information received from DND. The Investigator noted that the Incident raised "significant concerns towards the subject's judgment and trustworthiness" and recommended that a review for cause interview be conducted pursuant to the *Standard*. The Investigator also suggested that the Applicant's security status be suspended pending an investigation.

[17] On November 30, 2022, the Acting Director notified the Applicant that a review for cause investigation would be initiated pursuant to Appendix D of the *Standard*, and that his Reliability status was suspended pending completion of the review [Interim Suspension Decision]. He was also informed of his rights of redress in respect to this decision, namely that he "may complain to the Canadian Human Rights Commission, or the Federal Court."

[18] PSPC initially decided to postpone an interview with the Applicant until it received the results of DND's technical analysis. Due to significant delays, it later chose to conduct an initial security screening interview, with a follow-up interview to take place after DND provided its technical analysis. The screening interview was scheduled for May 25, 2023. The Applicant was notified that it would focus on the "November 2022 security incident" as well as his "past, including associations, previous employment, personal conduct, travel, any criminality, military service, etc."

(1) May 2023 Screening Interview

[19] During the May 25, 2023, interview, the Investigator discussed the substance of the Incident with the Applicant, including that DND detected a potential exploit program, Mimikatz, on a device that the Applicant inserted into his DWAN workstation. The Applicant stated he was familiar with Mimikatz but denied that it was present on any device that he may have inserted into his DWAN workstation.

[20] The Applicant and the Investigator discussed whether the Applicant had surrendered the correct device to DND investigators when he was confronted about the Incident. The Applicant said he had the actual device used during the Incident at his home. He agreed with the Investigator that it was important DND be notified, as this information was pertinent to DND's technical analysis of the Incident. The Applicant suggested it would be preferable for the Investigator to notify DND on his behalf because he is a *"persona non grata"* at DND.

[21] The Applicant also disclosed other information that was deemed relevant to and therefore was considered in PSPC's review for cause investigation, including:

- When asked if he had "conducted any work at all" since his security status was suspended, the Applicant disclosed having provided "assistance on technical issues" to "friends" at DND, which he conceded he "probably shouldn't have" done;
- In 2003, the Applicant got "into trouble" for inserting a personal USB device which had the capability to be used for "nefarious purpose" into his "DDPNI" computer. The Applicant had sourced this device from outside of DND and was warned at the time that the incident may affect "his ability to get future employment with the Army";
- At some point between August or September 2022, the Applicant mistakenly inserted a "Raspberry-Pi Microcontroller" (the Trinkey) which he had personally obtained from an online retailer into his DWAN workstation. The Applicant conceded that

inserting any personally obtained device into his classified workstation "might not have been… okay with DND" and that he should have reported this incident but did not do so; and

- The Applicant was aware from at least December 2022 that he had surrendered the wrong device to DND but made no effort to inform them or the Investigator.

(2) Post-Screening Interview

[22] Following the May 25, 2023, interview, the Applicant provided further information to PSPC by email on May 26, June 2, and June 13, 2023. He offered further explanation for the relevant device and indicated that it seemed to resemble a generic flash drive.

[23] On September 18, 2023, PSPC received a report containing DND's technical analysis of the Incident [Technical Report]. The Technical Report noted that an exploit was detected on the DWAN on November 15, 2022, and identified the Mimikatz tool as the source of the exploit. Although the Technical Report identified the serial number for the specific device containing Mimikatz, it was noted that this device had not been recovered from the Applicant. The Technical Report concluded that although "there was no evidence of running the Mimikatz executable file, the exposure via the existence of potentially malicious software on a DWAN host – was a direct breach of DWAN Information Systems Security Orders and led to the deactivation of the user's DWAN credentials."

[24] The Investigator contacted the Applicant on September 28, 2023, to schedule a subsequent review for cause interview on October 3, 2023.

(3) October 2023 Follow-up Interview

[25] At the beginning of the October 3, 2023, interview, the Applicant noted that he "was not aware of what brought [him] to the investigation process exactly." He was reminded that the follow-up interview was because PSPC had been waiting on the Technical Report from the DND. The Applicant was then given a copy of the Technical Report for his interpretation.

[26] After reviewing the Report and noting the device's serial number and that it was a "mass storage device," the Applicant determined that the device containing Mimikatz was the Flash Drive and not the Trinkey.

[27] PSPC did not ask the Applicant to surrender the Flash Drive for examination.

(4) Statement of Adverse Findings and Response

[28] On October 31, 2023, the Investigator notified the Applicant that PSPC was considering the revocation of his security status. The Applicant was advised that a Statement of Adverse Findings [SAF] would be provided to him by email and that he would be given an opportunity to respond to the SAF prior to a recommendation being presented to the final decision-maker.

[29] The Applicant made multiple email inquiries about the contents of the SAF before providing his final written response on November 28, 2023. Among other things, his final response reiterated that the device he inserted into his DWAN workstation on November 15, 2022, was the Flash Drive. He also claimed, for the first time in the investigation, that DND had provided this device to him.

[30] The final Investigation Report, dated January 12, 2024, recommended that the Applicant's security status be revoked based on the existence of "reasonable grounds to believe that the [Applicant] may exhibit behavior [*sic*] that would reflect negatively on his ability to protect government of Canada assets and information."

III. Decision Under Review

[31] On January 12, 2024, the Applicant received a letter from the Acting Director informing him of PSPC's decision to revoke his security status and outlining its investigation process.

[32] The Decision acknowledged the Applicant's response to the SAF, but concluded that "outstanding security concerns remain." The Decision listed seven factors which "have led to a negative appraisal of [the Applicant's] honesty, trustworthiness and overall reliability":

1. He "intentionally used an unauthorized personal device [the Trinkey] on DND assets";
2. His explanation for not discussing his intentions with his Chain of Command (he did not feel they would "understand") was considered "unacceptable";
3. His actions led to the "DWAN being exposed to a malicious software, which was determined by DND to be a breach of their security";
4. He should have been reasonably aware that his actions were unacceptable given his several years' experience as a contractor with DND and his disclosure of "having been cautioned by colleagues regarding [his] course of action" and "having been reprimanded in the past (circa 2003) for an incident of a similar nature";
5. He did not immediately report to DND security of the Trinkey insertion despite knowing he ought to;
6. He "provided the incorrect device to DND for assessment (allegedly by mistake) and did not make any attempt to contact them regarding this error", and his explanation was "assessed as unreasonable given the context";

7. Despite “being under the impression” he was “not authorized to communicate with DND personnel,” he “disclosed having done so.”

[33] The Decision concluded that “sufficient information exists to show that you cannot be relied upon to preserve the trust you have or may have been afforded. Therefore, a decision has been made to revoke your Reliability Status, thus administratively closing your Secret and Top-Secret clearance.”

IV. Issues and Standard of Review

[34] The parties agree that the issues are whether the Decision is reasonable and made in a procedurally fair manner. However, the Respondent identifies that one of the Applicant’s procedural fairness arguments is in relation to an interim decision and not the final decision that is under review.

[35] The parties agree and I concur that the procedural fairness arguments are to be reviewed on a standard of correctness or akin to correctness (*Canadian Pacific Railway Company v Canada (Transportation Agency)*, 2021 FCA 69 at paras 46–47 [*Canadian Pacific*]; *Schofer v Attorney General of Canada*, 2025 FC 50 at para 15; see also *Canadian Association of Refugee Lawyers v Canada (Immigration, Refugees and Citizenship)*, 2020 FCA 196 at para 35), for which “the ultimate question remains whether the applicant knew the case to meet and had a full and fair chance to respond” (*Canadian Pacific* at para 56).

[36] The merits of the Decision are to be reviewed on the standard of reasonableness (*Canada (Minister of Citizenship and Immigration) v Vavilov*, 2019 SCC 65 at paras 16-17, 23-25, 85, 99, 101-4, 115-26 [*Vavilov*]).

[37] A reasonable decision is "based on an internally coherent and rational chain of analysis" and is "justified in relation to the facts and law that constrain the decision-maker" (*Vavilov* at paras 85–86; *Canada Post Corp v Canadian Union of Postal Workers*, 2019 SCC 67 at paras 2, 31). A decision will be reasonable if, when read as a whole and taking into account the administrative setting, it bears the hallmarks of justification, transparency, and intelligibility (*Vavilov* at paras 91–95, 99–100).

V. Submissions

[38] The Applicant argues the Decision is unreasonable. He also argues it was arrived at in a procedurally unfair manner, both due to bias and because he was not informed of the case against him or given a meaningful opportunity to respond.

[39] The Respondent maintains the Decision is reasonable and the procedural fairness protections afforded to the Applicant in PSPC's investigation went above and beyond what was required.

A. *Preliminary Issue: Interim Suspension Decision*

[40] The Respondent takes the position that the Applicant's allegations of bias concerning the Interim Suspension Decision dated November 30, 2022, are not properly before the Court. Rule

302 of the *Federal Courts Rules*, SOR/98-106 [*Rules*] instructs that "[u]nless the Court orders otherwise, an application for judicial review shall be limited to a single order in respect of which relief is sought."

[41] The Respondent submits the Applicant could have challenged the Interim Suspension Decision on judicial review but did not.

[42] The Respondent implicitly suggests no exceptions to Rule 302 have been established (see *Huang v Canada (Public Safety and Emergency Preparedness)*, 2015 FC 28 at para 80 [*Huang*]; *Granados v Canada (Citizenship and Immigration)*, 2018 FC 302 at para 36).

[43] At the hearing, the Applicant submitted that he is not trying to challenge a different decision, but rather that the DND's portrayal of the Applicant to PSPC tainted the entire process (outlined in more detail below). The Applicant submits it is entirely proper to raise remarks made by the DND in this context.

B. *Procedural Fairness of the Investigation*

(1) Reasonable apprehension of bias

[44] The Applicant submits that the DND Analyst who managed the Applicant's file and was responsible for communications between DND and PSPC [Analyst] demonstrated bias throughout the investigative process, and "[a]s a result, the entirety of the Review for Cause process has been tainted."

[45] The Applicant alleges that the Analyst pre-judged his matter before the investigation started, referencing DND's November 28, 2022, correspondence to a PSPC employee asking that the Applicant's security clearance be suspended during the investigation due to his "very poor judgment." The Applicant takes issue with the DND's comment that the Applicant "confirmed deliberate use of an exploitation toolset on the DWAN and appears unrepentant" for similar reasons.

[46] As noted above, the Respondent submits the interim suspension decision is not properly before this Court. However, in the alternative, the Respondent submits that the Applicant's assertions of bias are without merit and "based on an incorrect characterization of the decision-making process." The Respondent stresses that Interim Suspension Decision was made by PSPC, not DND, and that "there is no basis on which this Court could find that allegedly biased comments made by a DND analyst who had no authority to direct PSPC could have tainted PSPC's decision."

[47] The Respondent submits that PSPC conducted an independent assessment based on the information available, and the Interim Suspension Decision was justified both in its own right and by the comprehensive NAIR, which "did not cite DND analyst's comments in support of the recommendation to suspend of the Applicant's security clearance pending a review for cause investigation." Further, the Interim Suspension Decision was not tantamount to a final decision on PSPC's review for cause investigation, per the *Standard*.

(2) Participatory Rights

[48] In addition to his allegation of bias, the Applicant submits the Review for Cause Investigation was procedurally unfair for two reasons: (1) the May 2023 interview was completed based on a wrong assumption as to which device was actually involved in the matter, and (2) the investigative delay resulted in a "fishing expedition" in the May 2023 interview.

[49] First, the Applicant submits that DND was aware as early as December 2022 that it had not retrieved the correct device (the Flash Drive), but did not alert him or PSPC or give him an opportunity to provide it for testing before finalizing the Technical Report. He alleges this led the May 2023 interview to be "based on a fundamentally wrong assumption as to which device (and which insertion) was actually involved in the matter." The Applicant argues this caused him to be "unable to properly appreciate and respond to the allegations."

[50] The Applicant similarly alleges the May 2023 interview was used as a "fishing expedition" to solicit information from him. He points to how the Decision cites the 2003 incident, which "only became known to PSPC investigators through their broad and unfocused questioning at the May 25 interview." He alleges that had DND sent the Technical Report to PSPC earlier, the Investigator "would not have embarked on his broad-based endeavour to solicit inculpatory evidence from the Applicant." He also notes that the Investigator raised concerns with DND about the delay, meaning that "DND was therefore well aware of the prejudicial impact of its delay in communication, but still took no steps to provide the [Canadian Forces Network Operations Centre [CFNOC]] Technical Report to PSPC in a timely fashion."

[51] The Applicant argues he was owed a heightened level of procedural fairness because the Decision impacts his livelihood and no appeal procedure is provided by statute (*Baker v Canada (Minister of Citizenship and Immigration)*, 1999 CanLII 699 (SCC), [1999] 2 SCR 817 at paras 24–25).

[52] The Respondent submits that holding a security status is a privilege, not a right, and that the duty of procedural fairness owed to the Applicant is on the low end of the spectrum (*Tesluck v Canada (Attorney General)*, 2020 FC 1041 at para 20; *Sidoli v Canada (Attorney General)*, 2024 FC 1673 at paras 34, 38; *Henri v Canada (Attorney General)*, 2016 FCA 38 at paras 21-23 [*Henri*]; *Ritchie v Canada (Attorney General)*, 2020 FC 342 at paras 18, 3435; *Salmon v Canada (Attorney General)*, 2014 FC 1098 at para 46; *Koulatchenko v Financial Transactions and Reports Analysis Centre of Canada*, 2014 FC 206 at paras 98, 107; *Pouliot v Canada (Transport)*, 2012 FC 347 at para 10; *Rivet v Canada (Attorney General)*, 2007 FC 1175 at para 25; *Neale v Canada*, 2016 FC 655 at para 92).

C. *Reasonableness of the Decision*

[53] The Applicant also submits that the Decision is unreasonable for several reasons.

[54] First, he submits that the Acting Director unreasonably misconstrued the facts and overinflated the risk to the DWAN system. Notably, he argues that the Acting Director conflated the Trinkey with the Flash Drive (stating he "intentionally used an unauthorized personal device on DND assets") and therefore conflated two different insertion incidents. The Applicant maintains that the Flash Drive was an authorized device provided to him by DND. He points out

that the "Technical Report takes no issue with the Trinkey Device and did not identify it as problematic." He alleges that his mistaken insertion of the unauthorized Flash Drive cannot reasonably give rise to a finding of unreliability and untrustworthiness.

[55] The Applicant also submits that the 2003 incident did not result in any sanction, penalty, or reprimand, and that the Acting Director "over-inflat[ed] the outcome … without any evidence of such." He similarly argues that the Acting Director drew an unreasonable conclusion about his post-suspension communication with DND personnel. He maintains that the questions he answered were generic, and that he "did not discuss the security allegations and at no point did the Applicant initiate communications with DND personnel."

[56] The Applicant further argues that the Acting Director failed to meaningfully grapple with his submission that he "purchased the Trinkey device in an attempt to mitigate a genuine problem."

[57] Finally, the Applicant submits that the importance of the decision to his livelihood requires the Decision's reasons to reflect the stakes (*Vavilov* at para 133; *Mason v Canada (Citizenship and Immigration)*, 2023 SCC 2 at para 74). He alleges the Decision has "retired [him] against his will" and "may impact his ability to travel outside the country." He submits that the Decision fails to grapple with the consequences to him.

[58] The Respondent submits the Decision is reasonable and that the Applicant is asking the Court to reweigh and reassess the evidence, which is not its role on judicial review (*Vavilov* at para 125).

[59] The Respondent submits PSPC did not err by conflating the Trinkey and Flash Drive. The Respondent emphasizes that "the core security concerns raised by PSPC's investigation into the Incident — that the Applicant had exposed the DWAN to a tool capable of malicious actions (the Flash Drive containing the Mimikatz tool) *and* had inserted an unauthorized, personally obtained device into his DWAN workstation (the Trinkey device) — were central to PSPC's decision" [emphasis in original].

[60] The Respondent further argues that the Applicant's "suggestion that the decision-maker erred by failing to consider that the Flash Drive was an 'authorized device' because DND provided it to him misses the point," which is that 1) he was aware Mimikatz could be used for malicious purposes, 2) he transferred Mimikatz onto the Flash Drive before the Incident, and 3) this was a breach of numerous rules and policies governing his use of DND assets.

[61] The Respondent also points out that the Applicant volunteered information concerning the 2003 incident and his post-suspension communications with DND colleagues. The Respondent submits it was open to PSPC to consider this information. In particular and under the circumstances, the post-suspension communications were "a further example of the Applicant's flippant attitude towards departmental security orders, which contributed towards the negative appraisal of his overall trustworthiness as a Reliability Status and Top-Secret clearance holder."

VI. Analysis

A. *Preliminary Issue: Interim Suspension Decision*

[62] I agree with the Respondent that the Interim Suspension Decision is not properly before this Court. The Interim Suspension Decision specifically set out the Applicant's avenues to challenge that decision, but the Applicant did not take either of them. It would be improper to now allow the Applicant to collaterally attack that decision during the review of a different decision (Rule 302 of the *Rules*; *Huang* at para 80). As such, any arguments attacking the procedural fairness of the Interim Suspension Decision are rejected.

[63] The Court has recognized an exception to Rule 302 where the matter is ongoing or forms part of a "continuous course of conduct" (see *Gagnon v Bell*, 2016 FC 1222 at para 35; *David Suzuki Foundation v Canada (Health)*, 2018 FC 380 at para 164; *Mahmood v Canada*, 1998 CanLII 8450 (FC) at para 10, *Truehope Nutritional Support Ltd v Canada (Attorney General)*, 2004 FC 658; *Khadr v Canada (Foreign Affairs)*, 2004 FC 1145). This may be the case where the impugned decisions are closely related and stem from the same series of events (see *Anichinapéo v Papatie*, 2014 FC 687 at para 29; *Shotclose v Stoney First Nation*, 2011 FC 750 at para 64).

[64] I find that no exception to Rule 302 exists in this case. Though the Interim Suspension Decision stemmed from the Incident, it was completed by a separate department for a different purpose than the Decision. In my view, the Interim Suspension Decision is not sufficiently

closely related to qualify as a continuous course of conduct. Regardless, as will be explained below, the Decision did not rely on the comments of the Interim Suspension Decision.

B. *Procedural Fairness of the Investigation*

(1) Reasonable apprehension of bias

[65] Notwithstanding the above, I agree with the Respondent that no reasonable apprehension of bias arises in this case.

[66] The test for determining reasonable apprehension of bias is whether an informed person, viewing the matter realistically and practically, and having thought the matter through, would think it more likely than not that the decision-maker would unconsciously or consciously decide the issue unfairly (*Committee for Justice and Liberty et al v National Energy Board et al*, 1976 CanLII 2 (SCC) at 394). A reasonable apprehension of bias will arise when there has been a prejudgment of the matter to such an extent that any representations to the contrary would be futile (*Newfoundland Telephone Co v Newfoundland (Board of Commissioners of Public Utilities)*, 1992 CanLII 84 (SCC), [1992] 1 SCR 623 at 638).

[67] An allegation of bias against an administrative decision-maker is serious and "cannot rest on mere suspicion, pure conjecture, insinuations or mere impressions of an applicant or his counsel"; rather, such an allegation "must be supported by material evidence demonstrating conduct that derogates from the standard" (*Arthur v Canada (Attorney General)*, 2001 FCA 223 at para 8).

[68] That being said, I find that the comments made by DND do not raise a reasonable apprehension of bias because the Applicant has not established a connection between them and the two other alleged breaches of procedural fairness outlined above. Indeed, the Applicant explicitly stated that the subsequent investigation "breached the Applicant's right to procedural fairness in two further ways" [emphasis added], suggesting that the other alleged breaches are separate.

[69] Furthermore, PSPC, the decision-maker for the application under review, never quoted these allegedly biased comments. The Investigation Report included DND's infographic, but I find based on both the Investigation Report and the final Decision that the PSPC did its own assessment, primarily referring to the contents of the interviews with the Applicant.

(2) Participatory Rights

[70] I agree with the Respondent that the procedural fairness owed to the Applicant in the case at bar was on the low end of the spectrum, per the caselaw cited above. In my opinion, procedural fairness was accorded in this case.

[71] As noted above, procedural fairness requires that applicants know the case against them and have an opportunity to respond (*Canadian Pacific* at paras 46–47). In the case at bar, I find that the Applicant knew the case to meet during the May 2023 interview. As pointed out by the Respondent, at the time of his interview, the Applicant had been aware for several months of the primary concern which led to the interim suspension of his security status and the review for cause investigation. Indeed, on November 30, 2022, he was informed by the Interim Suspension

Decision of PSPC's concern that he had inserted a device which contained a "credential stealing tool" into his DWAN workstation. The Applicant also admitted in the May 2023 interview that he was already aware that he may have surrendered the wrong device.

[72] Furthermore, it is noted in the Investigation Report noted that PSPC's decision to conduct this interview before having received the Technical Report from DND was to the Applicant's benefit from a procedural fairness perspective. During the interview, the Applicant himself expressed to the investigator his appreciation for having been giving that opportunity.

[73] Also, prior to the interview, the Applicant was given advance written notice that it would cover the Incident itself as well as his past, including associations, previous employment, personal conduct, travel and any criminality, military service, etc. He was reminded so before the start of the interview and agreed to answer the questions. As stressed by the Respondent, the Investigation Report notes that the May 25, 2023, interview was conducted using a standard interview questionnaire as a guide and that such topics are expected to be covered in any security interview conducted pursuant to the *Standard*. According to the *Standard*, a review for cause is a reassessment of an individual's eligibility to hold a security status or clearance previously granted. This requires that an investigation and security interview be conducted which must consider background information leading up to the relevant security incident. No decision flowed from the May 2023 interview and the Applicant was provided with numerous other opportunities to provide information, including an October 2023 follow-up interview after PSPC received DND's Technical Report and his submissions on the SAF which were considered in PSPC final decision under judicial review.

[74] Many of the Applicant's arguments on the issue of procedural fairness take issue with the actions and procedure of DND, which, as outlined above, was not the decision-maker in this case.

[75] As the Federal Court of Appeal explained in *Henri* at paragraph 35, procedural fairness demands only that persons in this situation are provided with a meaningful opportunity to respond to the evidence against them, and for that response to be considered. For the reasons mentioned above, I find that is what happened in this case.

C. *Reasonableness of the Decision*

[76] I agree with the Respondent that the Decision was reasonable. The Applicant is asking this Court to re-weigh and reassess the evidence (*Vavilov* at para 125) and engage in an impermissible "line-by-line treasure hunt for error," which is not its role on judicial review (*Vavilov* at paras 125, 102).

[77] There is ample evidence in the record to justify PSPC's decision, and the reasons provided by the decision-maker are responsive to that evidence.

[78] Contrary to the Applicant's argument, no unreasonable conflation of evidence was demonstrated. While the decision-maker did not use the term "Pico," it considered the two actions conducted by the Applicant distinctly. The Decision clearly states that the security concerns raised by PSPC's investigation into the Incident are that: 1) the Applicant had exposed the DWAN to a tool capable of malicious actions: (the Flash Drive containing Mimikatz); and 2)

he had inserted an unauthorized, personally obtained device into his DWAN workstation (the Trinkey). Both actions were central to PSPC's decision to revoke the Applicant's security clearance.

[79] Reasonableness review is not a "line-by line treasure hunt for error" (*Vavilov* at para 102) and that written reasons "must not be assessed against a standard of perfection" (*Vavilov* at para 91). Reasons are to be "read holistically" and "in conjunction with the record." (*Vavilov* at para 103).

[80] Furthermore, counter to the Applicant's argument that the decision-maker relied on an "error" in the final Investigation Report that the relevant device was the Trinkey (because of the use of the term "Pico"), the summary of the CFNOC Technical Forensic Report quoted in the Investigative Report defined the "Pico" by the USB serial number that matched that of the Flash Drive containing the Mimikatz (21BABE06).

[81] The Applicant is a software engineer with over 35 years of experience in security contracting. Thus, he ought to have been aware that the use of any personal device on any DND asset without approval was not authorized. The record indicates that when DND officials are hired or contacted, they are advised that any usage of such a device required advance approval from DND. The Applicant failed to obtain approval prior to using the Trinkey despite being obligated to do so. According to his own declaration to the PSPC investigator, he discussed the use of the device with colleagues, who thought it was a bad idea. As pointed out by the Respondent, at the request of PSPC, DND officials identified several internal policies and security orders that the Applicant contravened to by using this personal device.

[82] Furthermore, I agree with the Respondent that the Applicant's assertion that the Decision failed to consider that the Flash Drive was an "authorized device" because DND provided it to him misses the point — the Applicant recognized, having transferred the Mimikatz tool, that could be used for malicious purposes onto the Flash Drive prior to November 15, 2022. This was clearly a breach of various rules and policies governing the Applicant's use of DND assets and it was reasonable for the Decision to find that this justified the revocation of his Reliability status.

[83] Regarding the 2003 incident, I find that it was reasonable for the decision-maker to have considered it given that the Applicant volunteered this information to the PSPC investigator during the May 25, 2023, interview and that it was relevant to the review for cause according to the *Standard*. I agree with the Respondent that the Applicant's description of the informal admonishment he received as a result of the 2003 incident is compatible with the use of the word "reprimand"; the Applicant himself described having gotten into trouble as a result of this incident and having been warned that it could impact his ability to be employed by the Canadian Armed Forces in the future.

[84] Finally, I find that the Applicant has not demonstrated that PSPC drew unreasonable conclusions from his having spoken to colleagues during his interim suspension while being under the impression that he was not authorized to do so by DND. It was reasonable for PSPC to consider the Applicant's dismissive attitude and his disregard of these instructions when evaluating his overall trustworthiness as a Reliability Status and Top Secret clearance holder.

[85] In my view, it was only after a comprehensive investigation, including two interviews, as well as an analysis of the evidentiary record that the PSPC decided to revoke the Applicant's Reliability status. The Decision was both procedurally fair and reasonable.

VII. Conclusion

[86] For the above reasons, this application for judicial review is dismissed. The Applicant has not raised any reviewable errors warranting the intervention of this Court.

VIII. Costs

[87] The Court has full discretionary power over the amount and allocation of costs, per Rule 400 of the *Rules*. As a general principle, the successful party is entitled to its costs (*Cozak v Canada (Attorney General)*, 2023 FC 1571 at para 30).

[88] The Applicant asks to pay a lump sum of $1,000 if his application is dismissed while the Respondent argues that an amount of $3,600 is justified.

[89] The Applicant has lost his long-term employment and appears to have brought this application for judicial review in good faith. Given the circumstances, I agree with the Applicant that $1,000 in lump sum costs is a reasonable amount.

JUDGMENT in T-258-24

THIS COURT'S JUDGMENT is that:

1. The application for judicial review is dismissed.

2. The Applicant shall pay the Respondent $1,000 in all-inclusive lump sum costs.

"L. Saint-Fleur"
Judge

FEDERAL COURT

SOLICITORS OF RECORD

DOCKET:	T-258-24
STYLE OF CAUSE:	KIMBERLY MUMA v ATTORNEY GENERAL OF CANADA
PLACE OF HEARING:	OTTAWA (ONTARIO)
DATE OF HEARING:	MAY 6, 2025
JUDGMENT AND REASONS:	SAINT-FLEUR J.
DATED:	AUGUST 12, 2025

APPEARANCES:

Malini Vijaykumar Emma Lodge	FOR THE APPLICANT
Taylor Andreas	FOR THE RESPONDENT

SOLICITORS OF RECORD:

Nelligan O'Brien Payne LLP Barristers and Solicitors Ottawa (Ontario)	FOR THE APPLICANT
Attorney General of Canada Ottawa (Ontario)	FOR THE RESPONDENT