Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 197-2022, 215-2022

Ministry of Corrections, Policing & Public Safety

April 26, 2023

Summary: The Ministry of Corrections, Policing and Public Safety (Corrections) proactively reported a breach of privacy to the Commissioner's office. Approximately 55 Corrections employees had inappropriately accessed the personal information and personal health information of two individuals connected to the Regina Correctional Centre. Corrections notified the Complainant, who was not satisfied with Corrections' response to the breach and proceeded to file a formal complaint with the Commissioner's office. The Commissioner investigated the incident and found that Corrections' notice to the Complainant was not adequate, and it did not take adequate steps to contain and investigate the breach. The Commissioner also found that Corrections' plan to prevent further breaches was not adequate. The Commissioner recommended Corrections amend its breach containment and investigation practices. The Commissioner also recommended that Corrections implement a proactive random sampling/audit schedule for CJIMS users and report back its compliance within 60 days of receiving this Investigation Report.

I BACKGROUND

[1] On October 18, 2022, the Ministry of Corrections, Policing and Public Safety (Corrections) proactively reported a breach of privacy to my office. In its report to my office, it indicated that a Corrections Officer at the Regina Correctional Centre (RCC) had lodged an internal complaint alleging that an unknown number of employees at RCC had viewed her ex-partner's (an inmate) records periodically since May 2020 in the Criminal Justice Information Management System (CJIMS). The information accessed was both the Corrections Officer's and her ex-partner's. Upon completion of an audit, Corrections was

able to confirm that several RCC employees had viewed her ex-partner's records without a legitimate business reason to do so.

[2] By way of letter dated October 20, 2022, Corrections notified one of the affected individuals (the ex-partner) of the breach of privacy. It notified the second affected individual (the Corrections Officer) of the privacy breach verbally during a meeting on October 17, 2022.

[3] On October 25, 2022, my office notified Corrections that it would be investigating the matter and requested Corrections provide further details of the privacy breach by November 23, 2022. On October 27, 2022, Corrections provided my office with a copy of its internal investigation report and supplementary information on March 1, 2023, April 14, 2023 and April 20, 2023.

[4] On November 9, 2022, my office received a complaint from one of the affected individuals (the ex-partner) as they were not satisfied with the investigation conducted by Corrections. When a complaint is received from an affected individual following a proactively reported breach, my office automatically issues an investigation report on the matter.

[5] On December 7, 2022, my office notified the affected individual (the ex-partner, hereinafter referred to as the Complainant) that my office would be investigating the matter.

II DISCUSSION OF THE ISSUES

1. Do I have jurisdiction?

[6] Corrections qualifies as a "government institution" pursuant to subsection 2(1)(d)(i) of *The Freedom of Information and Protection of Privacy Act* (FOIP).

[7] I will first consider whether personal information is involved pursuant to FOIP. For the privacy provisions of Part IV of FOIP to be engaged, the information at issue must constitute "personal information" as defined by subsection 24(1) of FOIP (IPC *Guide to*

FOIP, Chapter 6: "Protection of Privacy", updated: February 27, 2023, at page 31 (*Guide to FOIP*, Ch. 6, p. 31)).

[8] Corrections provided screenshots of the types of information accessed on CJIMS that would have been viewable on the Complainant. This includes name, date of birth, gender, address, photograph, court enforcement details (criminal history, non-contact orders), and drivers licence number. It appears the Corrections Officer was named in the Complainant's file, and so their name would be connected to information that relates to them. All of these data elements qualify as "personal information" as defined by subsections 24(1)(a), (b), (d), (e), and k(i) of FOIP which provide as follows:

> **24**(1) Subject to subsections (1.1) and (2), **"personal information"** means personal information about an identifiable individual that is recorded in any form, and includes:
>
> (a) information that relates to the race, creed, religion, color, sex, sexual orientation, family status or marital status, disability, age, nationality, ancestry or place of origin of the individual;
>
> (b) information that relates to the education or the criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved;
>
> …
> (d) any identifying number, symbol or other particular assigned to the individual, other than the individual's health services number as defined in *The Health Information Protection Act*;
>
> (e) the home or business address, home or business telephone number or fingerprints of the individual;
>
> …
> (k) the name of the individual where:
>
> (i) it appears with other personal information that relates to the individual; or

[9] Therefore, personal information is involved as defined by subsection 24(1) of FOIP, and FOIP is engaged.

[10] I must also consider whether *The Health Information Protection Act* (HIPA) is engaged as some of the data elements involved in this privacy breach may be "personal health

information". HIPA is only engaged if three elements exist: (1) there is a trustee within the meaning of subsection 2(t) of HIPA; (2) there is personal health information involved within the meaning of subsection 2(m) of HIPA; and (3) the personal health information is in the custody and control of the trustee at the time of the privacy breach.

[11] For the first element, Corrections is a trustee pursuant to the definition at subsection 2(t)(i) of HIPA. Subsection 2(t)(i) of HIPA provides:

> **2** In this Act:
> …
>
> (t) **"trustee"** means any of the following that have custody or control of personal health information:
>
> (i) a government institution;

[12] For the second element, Corrections indicated that the Complainant's health services number (HSN) can be viewed on CJIMS. A HSN qualifies as "personal health information" pursuant to subsection 2(m)(v) of HIPA which provides as follows:

> **2** In this Act:
> …
>
> (m) **"personal health information"** means, with respect to an individual, whether living or deceased:
>
> …
> (v) registration information;

[13] Finally, for the third element, as the Complainant's HSN is contained on CJIMS, and CJIMS is managed by Corrections, the HSN is in Corrections' custody or control. As all three elements are present, HIPA is also engaged in this matter.

[14] Therefore, I find I have jurisdiction to conduct this investigation pursuant to both FOIP and HIPA.

2. Did Corrections respond appropriately to the privacy breach?

[15] In circumstances where there is no dispute that a privacy breach has occurred, the focus for my office becomes one of determining whether the government institution or trustee has appropriately handled the privacy breach. To be satisfied, my office would need to be confident that Corrections took the privacy breach seriously and appropriately handled it.

[16] As set out in my office's *Rules of Procedure*, we will consider if Corrections followed the four best practices:

1. Contain the breach (as soon as possible)
2. Notify affected individuals (as soon as possible)
3. Investigate the breach
4. Take appropriate steps to prevent future breaches.

[17] In the following paragraphs I will analyze if Corrections followed these four best practice steps.

Contain the breach (as soon as possible)

[18] Upon learning that a privacy breach has occurred, government institutions and trustees should immediately take steps to contain the breach. Depending on the nature of the breach, this can include:

- Stopping the unauthorized practice
- Recovering the records
- Shutting down the system that has been breached
- Revoking access to personal information or personal health information
- Correcting weakness in physical security

(*Guide to FOIP*, Ch. 6, p. 273)).

[19] In my office's Review Report 154-2022, I stated at paragraph [27] that as part of analyzing containment, I want to conclude that reasonable steps were taken by the government institution or trustee to contain the breach. I want to have some reassurance the government institution or trustee has reduced the magnitude of the breach and the risk to affected individuals, such as risk to reputation.

[20] From the information provided to my office, the Corrections Officer first made a complaint about inappropriate access to personal information in CJIMS in May 2020. The complaint was made to the Deputy Director of Personnel at RCC. However, it appears that it took Corrections two years to notify its internal Privacy Unit of the alleged privacy breach. This resulted in no investigation being initiated until May 2022. This delay is very concerning and resulted in an open and ongoing breach of privacy for the two affected individuals. It is really important that Corrections' staff notify its privacy unit at the earliest opportunity after becoming aware of a risk of inappropriate behaviour that could involve personal information or personal health information. This allows Corrections to also conduct audits of information systems at the earliest opportunity after becoming aware of a risk of inappropriate behaviour.

[21] Once the Privacy Unit was advised, it conducted an audit of CJIMS in June 2022 and determined at that time 83 RCC employees had accessed the Complainant's records without a business purpose for doing so. However, some of those employees no longer work for Corrections. Upon further investigation, it was determined that some had a legitimate business purpose for accessing the personal information in CJIMS. As a result of these two factors, Corrections modified the number of employees with questionable access to the CJIMS to 55 employees. Corrections indicated that these 55 employees still needed to be interviewed as of April 14, 2023, which is almost a year after the audit was first conducted in June 2022. The delay in completing the investigation is unacceptable. Corrections has advised that access to CJIMS has not been revoked for any of the 55 suspected snoopers and it has not indicated that any additional monitoring of these employees' access to CJIMS is occurring while it slowly investigates.

[22] As a result of the **unacceptable delay** in completing an investigation (**3 years** since original complaint) and the fact that access to the personal information and personal health information is still available to the possible snoopers, I find that Corrections has not appropriately contained the breach.

[23] I recommend that Corrections complete this investigation within 60 days of the issuance of this Investigation Report and that access to CJIMS be immediately suspended for any employees suspected of snooping until the investigation is completed. Currently, that appears to be 55 employees at RCC.

Notify affected individuals

[24] Section 29.1 of FOIP requires that, if there was an unauthorized use or disclosure of personal information, government institutions notify the affected individual(s) where the "incident creates a real risk of significant harm" (*Guide to FOIP*, Ch. 6, p. 268).

[25] Section 29.1 of FOIP states:

> **29.1** A government institution shall take all reasonable steps to notify an individual of an unauthorized use or disclosure of that individual's personal information by the government institution if it is reasonable in the circumstances to believe that the incident creates a real risk of significant harm to the individual.

[26] Even where section 29.1 of FOIP does not apply, unless there is compelling reason not to, government institutions should always notify affected individuals of a privacy breach. It is also the approach that should be taken by trustees.

[27] Corrections indicated in its internal investigation report that based on the sensitivity of the personal information involved, the incident meets the "risk of significant harm" threshold as set out in section 29.1 of FOIP. As such, notification to affected individuals should occur in this case.

[28] It is important to notify affected individuals for several reasons. Affected individuals have a right and need to know to protect themselves from any harm that may result. Government

institutions and trustees may also want to notify organizations, such as, my office, law enforcement or other regulatory bodies that oversee professions.

[29] A notice to affected individual(s) should include:

- A description of the breach (a general description of what happened)
- A detailed description of the personal information involved (e.g., name, credit card numbers, medical records, financial information, etc.)
- A description of possible types of harm that may come to the affected individual because of the privacy breach
- Steps taken and planned to mitigate the harm and prevent future breaches
- If necessary, advice on actions the individual can take to further mitigate the risk of harm and protect themselves (e.g., how to contact credit reporting agencies)
- Contact information of an individual within the organization who can answer questions and provide information
- A notice that individuals have a right to complain to the IPC (provide contact information)
- Recognition of the impacts of the breach on affected individuals and, an apology

(*Guide to FOIP, Ch 6, pp. 274-275*)

[30] Corrections notified the Complainant of the breach via letter on October 20, 2022, and the Corrections Officer verbally on October 17, 2022. In Corrections' verbal notification to the Corrections Officer, it asserted that it confirmed the breach, provided a description of the breach (including the number of people who accessed their personal information without authority and the type of information breached), steps taken to mitigate (contain) the harm and steps taken to prevent similar privacy breaches in the future, disciplinary action taken, contact information of Corrections' privacy team and contact information for my office.

[31] In Corrections' written notification to the Complainant, it included a description of the privacy breach, an apology, a description of the personal information involved, Corrections' contact details, notice about the right to complain to my office, and steps taken

to prevent future breaches. Corrections did not provide the number of people who accessed the personal information of the Complainant, containment efforts, a description of the types of harm that might result from the breach or advice on how to protect against further harm. Therefore, the notification letter was deficient.

[32] Corrections should ensure its breach notices include more detail about risks involved and steps taken to mitigate risks. Corrections should also have informed the Complainant of any disciplinary measures taken against the snooping employees. It is also problematic that the notification is coming two years after the alleged breach was first reported in a situation where real risk of significant harm exists. Further, the investigation is not completed yet and the breach has not been contained.

[33] For the reasons set out above, I find that Corrections' notice to the Complainant was not adequate. This is especially the case as Corrections has determined that a real risk of significant harm could occur because of the breach. I recommend that Corrections review its notification practices and ensure that, in the future, it meets the requirements set out above. I also recommend that upon completion of the investigation, Corrections issue new notification letters to both affected individuals with accurate and complete information as noted in this section of my Report.

Investigate the breach

[34] After containing the breach and notifying affected parties, government institutions and trustees should conduct an internal investigation. An internal investigation is a methodical process of examination, inquiry, and observation including interviewing witnesses and reviewing documents. The purpose is to conduct a root cause analysis, which is a useful process for understanding and solving a problem. It seeks to identify the origin of a problem by using a specific set of steps and tools to:

- determine what happened
- determined why it happened
- figure out what to do to reduce the likelihood that it will happen again.

(*Guide to FOIP*, Ch. 6, pp. 269-271)

[35] On May 16, 2022, the Executive Director of Custody Services contacted the Privacy Unit (Audit, Information Management and Safety) to initiate an investigation regarding two complaints made by the Corrections Officer. The Corrections Officer alleged their privacy was breached periodically since May 2020 and noted the following two incidents:

a. Complaint #1: The Complainant alleged that an unknown number of employees at RCC viewed their ex-partner's (an inmate) records via CJIMS. The ex-partner had charges involving the Corrections Officer. The Corrections Officer alleged that none of the employees had a job-related purpose or legislated authority to access the ex-partner's CJIMS records.

b. Complaint #2: The Corrections Officer alleged that employees who viewed their personal information via the inmate's CJIMS records had circulated the information to other employees at RCC.

[36] In its internal investigation report forwarded to my office, Corrections indicated their investigation efforts and outcomes were as follows:

> A June 8, 2022, CJIMS audit report (from May 2020 to June 2022) revealed that 122 employees viewed the inmate's CJIMS record while he was not present at RCC – either not in custody or transferred to or located at the Saskatoon Correctional Centre (SCC) or Prince Albert Correctional Centre (PACC). Of these 122 employees, 83 were RCC employees with no apparent job-related purpose to view the inmate's information, 17 were RCC employees with a likely reason (e.g., admitting officers), and 22 were non-RCC employees (some from SCC, PACC, or managers at head office). The scope of this investigation is limited to RCC employees who viewed the inmate's records while the inmate was not present at RCC. In other words, it focused on 100 (83 + 17) RCC employees.
>
> This investigation report only examines complaint #1 – RCC employees accessing the complainant's ex-partner's CJIMS record without an apparent job-related purpose. There was not sufficient evidence gathered to assess the allegations of Complaint #2 – employees circulating [the Correction Officer's] personal information to other RCC staff – as no RCC employees were interviewed. The RCC employees were not interviewed as it was determined to address the complaints in a phased approach. It is recommended that the RCC leadership investigate the allegations behind complaint #2.

[37] Corrections' Privacy Unit's investigation included a review of privacy safeguards that were in place and concluded that they were adequate. It asserted:

- Physical tokens are required for all CJIMS users

- CJIMS uses multi-factor authentication based on a user password, random code generated by physical token and security clearance screening
- An on-screen pop-up banner is used to alert staff on appropriate use of the system when they log into CJIMS
- Training on privacy and acceptable use of CJIMS is provided
- Oath of Office and CJIMS Request for Access Agreements include information about appropriate use and disclosure of personal information

[38] Corrections determined there was a real risk of significant harm to affected individuals as follows:

> Information accessed relating to the inmate could pose a risk of hurt, humiliation, damage to reputation, or risk of identity theft or fraud. Information accessed relating to the [Corrections Officer] could pose a risk of hurt, humiliation, damage to reputation, and/or risk of physical harm or psychological impact.

[39] Corrections indicated it intends to interview each of the 55 employees on the CJIMS audit report and take appropriate disciplinary steps. As of the issuance of this Investigation Report, this does not appear to have been completed yet.

[40] Corrections concluded in its report that the privacy breach was a result of failure of its employees to comply with policy and/or training regarding snooping and acceptable use of CJIMS and the delay in conducting investigations earlier.

[41] I agree with Corrections that the cause of these breaches was a failure of Corrections' employees to comply with existing policy. This was the same issue I dealt with in Investigation Report 088-2022 also concerning Corrections and employees snooping on CJIMS. This is problematic in that if activity like this continues to occur and is not immediately addressed, it can create a culture of snooping. As noted earlier in this Investigation Report, I recommend Corrections complete this investigation within 60 days of the issuance of this Investigation Report.

[42] In the next part of this Investigation Report, I will discuss Corrections' mitigation efforts, taking into account the recommendations it stated it would undertake in Investigation Report 088-2022 issued in October 2022.

Take appropriate steps to prevent future breaches

[43] Once you contain a breach and identify a root cause, you want to recommend and implement solutions that help towards preventing the same type of breach from occurring again. Prevention is one of the most important steps. A privacy breach cannot be undone but a government institution or trustee can learn from one and take steps to help ensure that it does not happen in the future. To avoid future breaches, government institutions and trustees should make a prevention plan.

[44] As noted above, Corrections' report included recommendations about steps it could take to prevent future breaches. These steps are as follows:

> 1. Develop a technical safeguard in CJIMS that prompts users to input a reason code to access the various screens.
>
> 2. Prepare an all-staff email to remind employees not to snoop.
>
> 3. Explore the feasibility of implementing a random sampling/audit schedule for CJIMS users.
>
> 4. Develop an online refresher training course for employees that addresses snooping and the obligations surrounding acceptable and unacceptable CJIMS usage as well as their duty to protect confidential information under FOIP and HIPA.
>
> 5. Use a consistent script when new employees sign the CJIMS Authorized Access, Use and Restrictions Agreement to ensure that employees understand improper use of CJIMS.
>
> 6. Review the CJIMS Authorized Access, Use and Restrictions Agreement periodically to ensure compliance.
>
> 7. Open a dialogue with the Public Service Commission to revise the wording of the oath or Declaration of Office to ensure employees meaningfully understand appropriate and inappropriate use and disclosure of information. We suggest clear and direct language similar to: "Government databases must not be used to search for information on any person(s) for personal reasons."
>
> 8. Initiate a deeper look into the out-of-scope areas of this investigation, including but not limited to:

- RCC employees with no legitimate reason to access the inmate's records while he was at RCC;

- (potentially) excessive searches by employees with legitimate reasons to look at the information;

- expand the investigation to Saskatoon Correctional Centre (SCC) and Prince Albert Correctional Centre (PACC), the other facilities that housed the inmate.

9. Proactively report this incident to the Saskatchewan Information and Privacy Commissioner's Office (OIPC).

10. Follow up with RCC as to the lack of action taken when the potential privacy breach activity was first reported by the complainant.

[45] I agree with Corrections' steps to prevent future breaches. Subject to the comments below, I recommend that Corrections comply with the proposed steps it has laid out and complete them in a timely fashion.

[46] Corrections' steps numbered 2, 3 and 4 in paragraph [44] of this Investigation Report are similar to those reported by Corrections in my office's Investigation Report 088-2022 issued on October 21, 2022. In paragraph [44] of Investigation Report 088-2022, Corrections made the same three recommendations in that similar privacy breach which were as follows:

Number	**Recommendation**	**Proposed Action**	**Completion Target Date**
…	…	…	…
2	Develop additional policy and/or training that addresses the penalties associated with snooping in CJIMS and informs employees of their duty to protect personal information under FOIP and personal health information under HIPA.	Review Provincial Policy Information Management 902 - CJIMS Authorized Access, Use and Restrictions and determine if there needs to be updates to meet the following recommendations. The Audit, Information Management and Safety, Integrated	October 31, 2022 March 31, 2023

		Justice Services (IJS) has developed a refresher privacy course for the Ministry that will be available by the end of the fiscal year.	
…	…	…	…
5	Implement a random sampling/audit schedule for CJIMS users. Assign a resource to manage this function to ensure it is regularly completed.	The Audit, Information Management and Safety Branch, IJS, will work with the Strategic Systems and Innovation Branch within Corrections, Policing and Public Safety to explore CJIMS's audit functions.	March 31, 2023
6	Develop an online refresher training course for employees to refamiliarize themselves with the obligations surrounding acceptable and unacceptable use of personal information in CJIMS.	The Audit, Information Management and Safety Branch, IJS has developed a refresher privacy course for the ministry that will be available by the end of the fiscal year.	March 31, 2023

[47] On April 5, 2023, my office sent an email to Corrections asking it to indicate if the recommendations made in my office's Investigation Report 088-2022 had been completed. On April 13, 2023, Corrections indicated to my office it had met all the recommended deadlines outlined in my office's Investigation Report 088-2022.

[48] In paragraph [46] of my office's Investigation Report 088-2022, I recommended Corrections move forward with its proposed preventative measure of informing staff of the disciplinary measures taken against employees that are found to be snooping in CJIMS. I added a recommendation to that preventative measure as follows:

> [46] Corrections' recommendation number two should include a requirement to inform all staff of the disciplinary action taken against the employee for snooping. Corrections should inform its staff of specific examples of privacy breaches that have occurred within the organization and of the discipline that followed. Repeatedly reminding employees that there is no tolerance for unauthorized access to personal information and personal health information can deter and prevent privacy breaches.

[49] I reiterate my recommendation made in paragraph [46] of my office's Investigation Report 088-2022 in this matter also.

[50] Proactive random audits are an important measure to protect privacy of personal information and personal health information. Managed properly random audits can be effective in detecting and deterring privacy breaches. I note that Corrections had indicated the following preventive measures in my office's Investigation Report 088-2022 and in its recommended steps above at paragraph [44] of this Report:

Number	Recommendation	Proposed Action	Completion Target Date
5	Implement a random sampling/audit schedule for CJIMS users. Assign a resource to manage this function to ensure it is regularly completed.	The Audit, Information Management and Safety Branch, IJS, will work with the Strategic Systems and Innovation Branch within Corrections, Policing and Public Safety to explore CJIMS's audit functions.	March 31, 2023

[51] On April 18, 2023, my office followed up with Corrections to inquire whether the random audit schedule had been implemented and what that schedule would be (e.g., annual random auditing).

[52] Corrections responded on April 20, 2023, indicating as follows:

> …This item (a random sampling/audit schedule) is not implemented. This is detailed in the letter that is still waiting for legal review and further approvals. However, I can provide the following as to the progress of this item.
>
> All allegations of snooping are reviewed and investigated on a case-by-case basis since CJIMS does not have an automated function to detect snooping. The Ministry is not currently considering implementing this workplan item. However, it remains something the Ministry may consider implementing at a later date.
>
> In October 2022, the Ministry established a working group to evaluate and assess the capabilities of CJIMS to audit unauthorized use and to examine best practices in auditing employee access. To help determine best practices, this group reached out to both provincial and federal partners – for example, other provincial privacy offices across Canada, the Treasury Board of Canada Secretariat, the Canada Revenue Agency, etc. – to gather best practices on how they protect, audit, and limit access to sensitive, personal information. The findings of these meetings showed that education and training, as well as prompts and just-in-time reminders, were the most effective strategies to prevent snooping. In line with these findings, the Ministry has developed and implemented the following safeguards:
>
> - A reason-code drop down to access each CJIMS record; the reason code gets logged and helps identify unauthorized access
> - A pop-up window that provides just-in-time notification around proper use of information
> - A new and more visible privacy statement when users first sign into CJIMS
> - A new privacy refresher training course that addresses snooping
>
> The working group meets on an ongoing basis to continue to improve technical and administrative safeguards to limit unauthorized use of personal information.

[53] I find that Corrections' plan to prevent further breaches has some limitations. With the severity of the breach over two years, it does not appear prompts and training alone will be sufficient to deter workers from snooping. This is also the second breach of this nature that I have investigated. Also, since it is unclear what disciplinary actions were taken on employees who were found snooping, there should be a preventive measure that would be a stronger deterrent. I recommend that Corrections implement a random sampling/audit schedule for CJIMS users as a preventative measure.

III FINDINGS

[54] I find that I have jurisdiction to investigate this matter under both FOIP and HIPA.

[55] I find that Corrections' efforts to contain the privacy breach were not adequate.

[56] I find that Corrections' notification to the Complainant was not adequate.

[57] I find that Corrections' investigation of the privacy breach was not adequate.

[58] I find that Corrections' plan to prevent future breaches is inadequate.

IV RECOMMENDATIONS

[59] I recommend that Corrections complete its investigation into this matter within 60 days of the issuance of this Investigation Report and that access to CJIMS be immediately suspended for the 55 employees suspected of snooping until the investigation is completed.

[60] I recommend that Corrections amend its policy and procedure so that staff are required to report potential breaches of privacy immediately upon discovery.

[61] I recommend that Corrections review its notification practices and ensure that, in the future, it meets the requirements set out in my office's *Guide to FOIP, Ch. 6, pp. 274-275.* I also recommend that upon completion of its investigation into this matter, Corrections issue new notification letters to both affected individuals with accurate and complete information as noted in this Investigation Report.

[62] I recommend that Corrections implement a random sampling/audit schedule for CJIMS users as soon as possible as an effective preventative measure.

[63] I recommend that Corrections' development of additional policy and/or training that addresses the penalties associated with snooping in CJIMS should include specific examples of privacy breaches that have occurred within the organization and of the discipline that followed.

[64] I recommend that Corrections complete the proposed preventative actions described at paragraph [44] of this Report in a timely fashion and report progress back to my office within 60 days of the issuance of this Investigation Report.

Dated at Regina, in the Province of Saskatchewan, this 26th day of April, 2023.

Ronald J. Kruzeniski, K.C.
Saskatchewan Information and Privacy Commissioner