Chapter 48
Justice—Maintaining the Integrity of Offender Data

1.0 Main Points

The Ministry of Justice (Ministry) is responsible for tracking offenders in provincial correctional facilities and within the community (e.g., those offenders subject to bail). The Ministry uses an information management system to track release dates of prisoners. If information in its system is not accurate, offenders may be released from prison at the incorrect time.

By August 2015, the Ministry implemented four of the six recommendations we initially made in our 2012 audit of the integrity of offender data. It developed a risk-based audit plan for auditing offender data, ensured staff who access the system have signed confidentiality agreements, encrypted and patched the system based on threat and risk assessments, and provided routine reports to senior management related to offender release errors.

The Ministry needs to ensure supervisors review offender information entered by clerical staff, and unneeded system user access is removed promptly.

2.0 Introduction

As of August 2015, the Saskatchewan correctional system was responsible for 11,173 offenders with 1,833 offenders in custody and 9,340 offenders under community supervision.[1]

The Ministry uses the Criminal Justice Information Management System (CJIMS) to track offenders in provincial correctional facilities and within the community (for example, those subject to conditional sentence, probation, or bail). CJIMS tracks offender location, sentence lengths, incidents, risk or needs assessments for offenders, special programs (e.g. community training residences), and release dates. As of June 1, 2015, CJIMS replaced the Ministry's previous system called Corrections Management Information System (CMIS).

CJIMS is critical for the management and transporting of offenders. If offender release date information is not accurate, offenders may be let out of prison at the incorrect time. Also, the Ministry relies on the confidentiality, availability, and integrity of information in CJIMS to keep safe both offenders and law enforcement officers charged with their care.

Our *2012 Report – Volume 2* concluded that the Ministry did not have effective controls to maintain the integrity of offender data and included six recommendations. This chapter reports the results of our first follow-up on those recommendations.

To conduct this review engagement, we followed the standards for assurance engagements published in the *CPA Canada Handbook – Assurance*. To evaluate the

[1] Per Ministry of Justice officials (September 2015).

Ministry's progress towards meeting our recommendations, we used the relevant criteria from the original audit. The Ministry agreed with the criteria in the original audit.

We examined key documents, including policies and procedures, interviewed employees of the Ministry, and tested the timeliness of the removal of unneeded user access to CJIMS.

3.0 Status of Recommendations

This section sets out each recommendation including the date on which the Standing Committee on Public Accounts agreed to the recommendation, the status of the recommendation at August 31, 2015, and the Ministry's actions up to that date. We found that the Ministry had implemented four out of six of our recommendations.

3.1 Ministry Using Risk-Based Audit Plan

We recommended that the Ministry of Justice use an approved risk-based plan for auditing offender files and Corrections Management Information System[2] data. (2012 Report – Volume 2; Public Accounts Committee agreement June 17, 2015)

Status – Implemented

The Ministry created the Sentence Management team in 2008. The team undertakes annual audits on active offender files at various correctional facilities and Community Corrections offices. The audits review the accuracy of sentence calculations, and are designed to detect system errors before the release date. The Ministry considered sentence calculation errors to be the most significant in that they impact offenders' release dates. The audits also look for other errors such as missing documentation, incorrect alerts within CJIMS, or incorrect dates for warrants with no impact on the expected release date.

In 2014-15 and 2015-16, the Sentence Management team developed risk-based audit plans. These plans detail areas of high risk, and focuses the teams' audit work on those areas. Senior Ministry officials approved these plans.

3.2 Review Processes Continue to Need Improvement

We recommended that the Ministry of Justice implement processes to require verification of Corrections Management Information System data entry. (2012 Report – Volume 2; Public Accounts Committee agreement June 17, 2015)

Status – Partially Implemented

[2] Subsequent to our 2012 audit, the Ministry replaced Corrections Management Information System (CMIS) with CJIMS. The recommendation, although directed at CMIS, also applies to CJIMS.

In our 2012 audit, we highlighted the importance of work of the Sentence Management team in identifying errors in release dates and correcting them. We also noted that to fix the identified errors, the Sentence Management team either directly adjusted system data, or asked a probation officer or admitting staff to make the correction. At that time, the Ministry did not have a process to make sure the correction was made properly.

Since our 2012 audit, the Ministry changed its processes to require a second review of files and data changes. When the Sentence Management team asks a probation officer or admitting staff to make the correction to CJIMS, the Sentence Management team enters this request in its spreadsheet, and reviews to confirm the change was correctly made. For 2014-15 audits completed by the Sentence Management team that we reviewed, all files and data changes contained evidence of review by two individuals.

To reduce the errors prior to the Sentence Management team review, the Ministry developed a policy, which came into effect on September 1, 2014. The policy requires supervisors to confirm the data entered into the CJIMS by clerical staff matches the information on the individual's court order. Probation officers assigned to the individual must also review that the data within the CJIMS matches what is on the court order. All individuals who perform these levels of review must place their initials on the court order indicating they completed the review.

At August 2015, all staff were not yet following this policy. None of the ten court orders from community corrections offices that we reviewed contained either a supervisor's or a probation officer's initials. Consistent review of data entered into CJIMS will reduce the magnitude of errors.

3.3 Confidentiality Agreements Signed

We recommended that the Ministry of Justice ensure all required confidentiality agreements for Corrections Management Information System users are completed and signed. (2012 Report – Volume 2; Public Accounts Committee agreement June 17, 2015)

Status – Implemented

CJIMS utilizes two-factor authentication (i.e., a key fob is also required to log in). Until the Ministry has received a signed confidentiality agreement from an employee, the employee is not to be set up as a new user in CJIMS, or provided a fob.

Since our 2012 audit, the Ministry keeps a spreadsheet listing the signed confidentiality agreements received from system users. For 10 individuals, we verified that signed confidentiality agreements were on file.

3.4 User Access Removal Still Not Timely

We recommended that the Ministry of Justice follow its policy to ensure that unneeded Corrections Management Information System user access is removed on a timely basis. (2012 Report – Volume 2; Public Accounts Committee agreement June 17, 2015)

Status – Partially Implemented

The Ministry has developed a policy that requires employees to have their CJIMS access removed once they have left the Ministry. The Ministry also collaborated with the Ministry of Central Services to align deactivation of CJIMS users with network user access removal. The Ministry receives, on a regular basis, listings of employees who no longer require network access. It compares this listing to its CJIMS user listing to identify instances where CJIMS access needs to be removed.

However, in 2014-15, we found 3 out of 10 users tested did not have their CJIMS access removed or disabled on a timely basis. In one instance, one user did not have their access to CJIMS removed until 70 days after the last day of their employment with the Ministry. Not removing unneeded user access promptly increases the risk that an unauthorized person could gain system access and obtain confidential information about offenders or inappropriately modify CJIMS systems or data.

3.5 CJIMS is Encrypted and Patched

We recommended that the Ministry of Justice determine and monitor encryption, patching and logging requirements for the Corrections Management Information System based on a threat and risk assessment. (2012 Report – Volume 2; Public Accounts Committee agreement June 17, 2015)

Status – Implemented

A service provider hosts CJIMS (the software and the servers on which it resides) and the offender data it contains. CJIMS data is encrypted and software is maintained and patched on a regular basis. The system also has logs that track when and who updates/views a record in CJIMS.

As part of its threat and risk assessment processes, the Ministry hired a third party to electronically look for vulnerabilities (weaknesses or flaws) in the security of CJIMS when it upgraded to a new version of CJIMS. While this test did not identify any high risk issues, it noted a number of medium and low risk issues. The Ministry has addressed the medium risk issues. The Ministry has scheduled another test in fall 2016 to coincide with the next CJIMS upgrade.

3.6 Incorrect Release Date Risks Identified and Reported

We recommended that the Ministry of Justice provide senior management with routine reports that completely described the risk of incorrect offender release dates, how that risk is managed, and all inappropriate offender releases. (2012 Report – Volume 2; Public Accounts Committee agreement June 17, 2015)

Status – Implemented

At the completion of each sentence management audit, the Sentence Management team provided senior management with a summary report that highlighted all errors. In addition, at the end of the year (in conjunction with its next year's risk-based audit plan), the Sentence Management team gave the Associate Deputy Minister of Custody, Supervision, and Rehabilitation Services a summary of the results of all audits completed.

Also, the Ministry established the Release Error Review Committee (RERC) in January 2015. The RERC is composed of various members of senior Ministry management as well as a liaison from the RCMP F Division.[3] At its monthly meetings, the Committee facilitated round table discussions of release errors and how to mitigate related risks.

[3] RCMP "F" Division denotes those RCMP officers working in and around the Province of Saskatchewan.