Chapter 27
Control over Offender Information and Release Dates

1.0 Main Points

The Ministry of Justice (Justice) uses the Corrections Management Information System (CMIS) to track and manage offenders in provincial correctional facilities and in the communities. Provincial correctional facilities are used to hold offenders sentenced to periods in prison of less than two years and remanded offenders. This chapter describes our audit of Justice's controls to maintain its integrity of offender data in CMIS. Justice relies on offender information in CMIS being accurate and complete to ensure the safety of both the offenders and those charged with their care. CMIS is also used for allowing offenders to exit correctional facilities. If this information is not correct, offenders may be released from jail at incorrect times.

For the period January 1, 2012 to August 31, 2012, we found Justice did not have effective controls for maintaining the integrity of offender data in CMIS. The Ministry had not established security requirements for CMIS data, did not remove unnecessary user access to CMIS on a timely basis, and did not have all staff that access CMIS data sign confidentiality agreements. As a result, an unauthorized person could obtain confidential offender information or inappropriately modify offender data. Justice should also have processes to review the accuracy of all CMIS data entry and approve a risk-based plan for verifying that CMIS data is accurate. These process improvements are needed to mitigate the release of offenders from correctional facilities at the wrong time.

As of May 25, 2012, two ministers are jointly assigned the administration of *The Correctional Services Act*—the Minister responsible for Corrections and Policing, and the Minister of Justice and Attorney General.

2.0 Introduction

The Correctional Services Act (Act) outlines responsibility for the provision of correctional services and programs. These include assessment, supervision, treatment, training, control, custody, rehabilitation or reintegration of offenders. An offender is a person who has been charged with or convicted of an offence and who is bound by a committal order (i.e., a probation order or an order for committal to a correctional facility), and includes a person transferred to a court or a correctional facility. An offender on probation is ordered to follow certain conditions set by the court, under the supervision of a probation officer.

The Adult Corrections branch of Justice delivers a range of programs that provide for varying levels of care, control and supervision of adult offenders. These adult programs are delivered through two operational systems: Institutional Operations and Community Operations (see **Figure 1**).

Figure 1—Institutional Operations and Community Operations

Institutional Operations:

- Institutional Operations supervises offenders in correctional facilities (i.e., prisons). Offenders sentenced to a period in jail of less than two years serve their sentence in a provincial correctional facility. Offenders sentenced to two years or more serve their sentence in a federal penitentiary.
- There are four provincial correctional centres for provincially-sentenced and remanded offenders (a remanded offender is someone who has been charged with an offence and has been denied bail, is unable to meet the conditions of bail, or is unable to post bail).
- There are also two community correctional centres, four community training residences, and one correctional camp for offenders who are rated as low security risk.

Community Operations:

- Community Operations supervises offenders in the community.
- There are seven regions with seventeen regional offices responsible for supervising offenders on conditional sentence, probation or bail.

3.0 Correctional Management Information System

The Corrections Management Information System (CMIS) tracks offenders in provincial correctional facilities and within the community (for example, those subject to conditional sentence, probation or bail). CMIS tracks offender location, sentence lengths, incidents, risk or needs assessments for offenders, and special programs (e.g., community training residences).

According to Justice, as of June 2012, the Saskatchewan correctional system was responsible for 8,160 offenders: 1,623 in custody and 6,537 under community supervision.

CMIS is critical for the management and transporting of offenders. Justice relies on the confidentiality, availability, and integrity of this information to ensure the safety of both the offenders and the law enforcement officers charged with their care. CMIS is also used to track release dates for prisoners. If this information is not accurate, offenders may be let out of prison at the incorrect time.

3.1 New System under Development

In 2009-10, a business case was approved to develop a criminal justice information management system (CJIMS). The new system will integrate system information so that a complete, historical view of all of an offender's current information could be provided to authorized stakeholders. This "one offender, one file" view is needed because the current Saskatchewan justice system relies on paper and various systems to communicate critical pieces of information.

In 2010-11, Justice and the Information Technology Office partnered to work with an external vendor to modernize the four critical applications for court services (JAIN[1] – Justice Automated Information Network), PCPIC[2] – Provincial Court Payment Information Centre, adult corrections (CMIS) and young offender programs (SYOCAMS – Saskatchewan Young Offenders Case Administration Management System) into one combined system called CJIMS.

[1] JAIN is the provincial court system that tracks the accused through the court system.
[2] PCPIC tracks summary offence tickets and interfaces with JAIN if tickets are not paid in a timely fashion.

Justice intends to use CJIMS to have a single computerized system to replace the systems currently in use, two of which are 25-30 years old, and to provide efficiencies in gathering and sharing accused/offender information. Justice plans to have CJIMS fully implemented in 2014.

Our recommendations in Section 5.0 are applicable for the development and implementation of CJIMS.

4.0 Audit Objective, Scope, Criteria, and Conclusion

The objective of this audit was to assess whether the Ministry of Justice has effective controls to maintain the integrity of offender data in the Corrections Management Information System for the period from January 1, 2012 to August 31, 2012. Integrity means that data is complete, accurate, and useful.

To conduct this audit, we followed the *Standards for Assurance Engagements* published in the *CICA Handbook - Assurance*. To evaluate Justice's processes, we used criteria based on the work of other auditors and current literature listed in Section 6.0. Justice's management agreed with the criteria listed in **Figure 2**.

We based our findings on our examination of Justice's policies, processes, and training manuals. We also examined CMIS, offender files, reports from CMIS, attended an audit with the sentence management team, and observed offender releases.

Figure 2—Audit Criteria

To have effective controls to maintain the integrity of offender data in the Corrections Management Information System, the Ministry of Justice should:

1. **Accurately and consistently input offender data**
   - 1.1 Data preparation and entry is authorized and timely
   - 1.2 Necessary and relevant data is input
   - 1.3 Validity and completeness of data is checked

2. **Maintain offender data integrity and security during processing**
   - 2.1 Maintain data reliability during processing, transmission or exchange
   - 2.2 System changes and maintenance occur and are tested
   - 2.3 Security access controls protect the system and data from unauthorized alteration

3. **Generate reports with useful, complete and valid offender data**
   - 3.1 Reports are authorized
   - 3.2 Reports are verified
   - 3.3 Reports provide useful information
   - 3.4 Errors are rectified

We concluded that for the period from January 1, 2012 to August 31, 2012 the Ministry of Justice did not have effective controls to maintain the integrity of offender data in the Corrections Management Information System (CMIS). Justice needs to:

- **Establish encryption, patching, and logging requirements**
- **Review all CMIS data entry**

- **Approve a risk-based plan for verifying CMIS data and report to senior management on how the risk is being managed**
- **Remove unneeded user access to CMIS on a timely basis**
- **Have confidentiality agreements signed by staff who have access to CMIS**

Without such controls, someone could obtain confidential offender data or inappropriately modify systems or data. Also, these control improvements will help to mitigate the release of offenders in error.

In Section 5.0, we set out our key findings and recommendations for each criterion.

5.0 Key Findings and Recommendations

5.1 Review and Verify Data Entry

CMIS is used by Institutional Operations (correctional facilities) and Community Operations to access offender information, case management activities, sentence calculations, etc. CMIS is used by correctional staff in the day-to-day management of offenders. Staff in various locations constantly open, close, update, and modify information to the records of offenders in CMIS. Entry of data is time stamped which creates a log of all changes made in CMIS to each offender's record including the time the change was made and who made the change.

Proper documentation is required to admit an offender into a correctional institution. Signed warrants from the court accompany offenders who enter institutions and are used to update sentence information into CMIS. Warrant information is entered into CMIS by admitting staff on the same day the offender is admitted. An admitting supervisor reviews information entered into CMIS to ensure it is accurate. Court information is kept on the offender's file which is maintained in locked file cabinets or file rooms.

CMIS tracks offenders by a unique identifier. A photo is taken of each offender entering a correctional institution and saved in a database separate from CMIS. Photos are used to ensure correct offenders are let out at the time of release. Without having the photo available in CMIS along with the offender's name and unique identifier, there is increased risk that the wrong offender may be let out in error. Justice told us that with the development of CJIMS, photos will be integrated along with offender information.

For Community Operations, court orders are usually faxed and entered into CMIS by clerical staff. Probation officers working in Community Operations monitor offenders serving their sentence in the community or who are out on bail. Offenders are required to report to their probation officer on a specified basis. Court orders for community service are usually either conditional sentence orders (CSO), where an offender is sentenced to jail but is allowed to serve their sentence in the community with conditions, or probation orders, where the offender can remain in the community subject to conditions. Clerical staff for Community Operations often enter court order information in CMIS the day of or the day after the information is received. However, there is no review

of data entered by clerical staff. As a result, data entry errors may occur. For example, staff need to make sure they enter the date the court order was made and not the date it was signed. The court order date is the date an offender's sentence begins and entering it incorrectly will impact a release date. Court order information is kept on the offender's file which is kept in locked file cabinets.

Conditional sentence orders (CSO) that are breached are of higher risk of being incorrectly entered into CMIS. In the event an offender breaches a CSO, the time credited against the CSO is stopped until the violation has been addressed by the court. Therefore, if violations occur on a CSO, calculating the time served against a CSO and the release date becomes much more complicated. As a result, the Ministry developed a spreadsheet that tracks time served against a CSO to assist correctional staff in calculating the revised release date. The revised release date is then entered into CMIS. It is important that the expected release date is correct so the offender is let out of prison or stops being monitored by the probation officer on the correct date. However, CSO release dates continue to be incorrect in CMIS. For example, the Ministry's sentence management team (further described below) found that 14 out of 92 errors in the 2011 fiscal year related to conditional sentence calculations. The extent of the errors resulted in changes in release dates ranging from 1 to 32 days.

To help mitigate the risk of errors, Justice has established conditional sentence experts in each Community Operations region across the province. Probation officers are supposed to complete the spreadsheet and submit it to the conditional sentence expert for review. However, we were unable to see evidence that this review process is taking place.

To reduce the risk of errors occurring in both Community Operations and Institutional Operations, senior management has implemented training programs and manuals for staff to effectively perform their work. Management created several policies, training programs, and a sentence management team to reduce errors.

The sentence management team was created in 2008. The sentence management team undertakes annual audits on active offender files at various correctional facilities and Community Operations offices. The audits identify calculation and other errors, and attempt to identify errors before a release date has passed that may have been incorrect. Calculation errors impact offenders' release dates and are considered by Justice to be the most significant possible errors. Other errors include instances where documentation is missing, alerts within CMIS are incorrect, or warrants have been entered incorrectly but did not have an impact on the expected release date.

The sentence management team's scope of work has varied from year to year. For example, in some years, the sentence management team only looked at a percentage of the offender population in some correctional facilities. The sentence management team's scope for the period we audited included only active offender files from CMIS as of the date of the sentence team's examination. Therefore, there is a risk that the team does not identify and correct all errors for the year (i.e., for offenders with release dates falling between audit dates). We did not see an overall risk-based plan approved by senior management that specifies which offender files will be audited. A risk-based plan would outline the correctional facilities or Community Operations offices to be audited, for what timeframe, and for which offenders.

1. **We recommend the Ministry of Justice use an approved risk-based plan for auditing offender files and Corrections Management Information System data.**

For the audit period, we observed that the sentence management team identified errors in release dates. For example, for the 2011 fiscal year, the sentence management team found a 5.4% error rate for Institutional Operations. Without the sentence management team identifying errors, errors would not be caught and fixed and offenders may be released on inappropriate dates.

The sentence management team has various ways of making changes to CMIS data – sometimes asking the probation officer or admitting staff to make changes and other times making changes directly. We did not see a verification check of changes made to CMIS data by the sentence management team. Moreover, as described earlier, there was not evidence of consistent review of data entered by staff in Community Operations.

2. **We recommend that the Ministry of Justice implement processes to require verification of Corrections Management Information System data entry.**

The Ministry requires criminal record checks, oaths and confidentiality agreements for staff. It is appropriate that staff provide criminal record checks and agree to terms of appropriate use and access to confidential offender data. Criminal record checks and oaths were appropriately completed. However, we found that not all staff had confidentiality agreements signed and filed in their personnel files.

3. **We recommend that the Ministry of Justice ensure all required confidentiality agreements for Corrections Management Information System users are completed and signed.**

5.2 Keep Offender Data Secure

Username and password authorization is required to access CMIS and users are required to change their password every 90 days. There are a limited number of people who have the ability to set up new CMIS users. All new users are required to complete basic training. New users are set up in CMIS based on a user request form signed by an authorized supervisor. CMIS has appropriate roles and privileges established which give users the ability to only change data for offenders for whom they are responsible. For example, a probation officer in Weyburn can only update information about offenders in the Weyburn area. There are a limited number of users with full access to change all CMIS data and their changes are time stamped for accountability.

Justice has a policy that requires users to have their CMIS access removed once they have left Justice. However, Justice is not following this process. We found that 6 out of 12 users tested did not have their CMIS access removed or disabled on a timely basis. Some users continued to have access to CMIS five months after they had left Justice. Of these 6 users, 3 also still had an active ministry network account. This increases the risk than an unauthorized person could gain system access and obtain confidential information or inappropriately modify systems or data.

4. We recommend that the Ministry of Justice follow its policy to ensure that unneeded Corrections Management Information System user access is removed on a timely basis.

CMIS (the database and the server on which it resides) and the offender data it contains are hosted by a service provider, the Information Technology Office (ITO). Connections to CMIS are also managed by ITO. Justice does not have a process to monitor ITO and to ensure that patching, logging, monitoring and maintenance are effectively performed on the CMIS server and database. As a result, Justice does not know if the offender data is appropriately secured. We found patches were not being installed. Patches play an important role in fixing security vulnerabilities.

Justice does not encrypt CMIS network traffic or CMIS data stored on laptops and servers. Encryption transforms confidential data to make it unreadable to anyone except those authorized to see it. CMIS data travels on a shared network between ITO and computers at various Justice facilities. That shared network should be treated as untrusted, requiring the encryption of confidential data. Some Justice employees occasionally traveled with confidential data stored on their unencrypted laptops. If their laptop is lost or stolen, confidential data could get into the wrong hands. Encrypting the laptop hard drives that store confidential data helps protect them should physical security measures fail. Furthermore, Justice has not performed a threat and risk assessment of CMIS to ensure that data protection controls are adequate and implemented. Justice has not had ITO perform any vulnerability assessments for CMIS.

5. We recommend 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.

System changes required to CMIS are identified by Justice. Justice then submits a request to have the change made to ITO. Changes are then documented, developed, and provided to Justice for testing. Once a change is approved by Justice, ITO moves the changes from the test environment to operations.

5.3 Prepare Useful Offender Data

Staff at correctional facilities run reports in CMIS to perform their daily work and effectively manage offenders. CMIS is accessible to staff who require it and is available for reporting on a daily basis.

Correctional institutions rely on a report from CMIS together with written documentation (a count maintained by staff) to determine the status and the number of offenders in total in the facility at any given time. Reconciliations are done between the manual count log and CMIS on a regular basis throughout the day.

To identify offenders who should be released from a correctional facility the next day, an "exit list" is run from CMIS on a nightly basis. When court information has been reviewed to confirm the offender should be released, staff print a photo of the offender from another system separate from CMIS. The photo is used confirm the identity of the offender the morning of release.

If an offender has to be released from the correctional facility to make a court appearance, an offender return form accompanies the offender. This process began in 2010. An offender return form is used to document offender information from CMIS when an offender leaves a correctional facility (e.g., to go to court). This helps ensure that offenders who should be returned to a correctional facility for a sentence unrelated to the one being heard in court are returned. This form is provided to the escorting officer along with the offender. After the court appearance, the court clerk fills out the disposition section of the form. The offender return form is to be returned to the correctional facility as soon as possible whether the offender is released or not, usually accompanying the offender if the offender is returned to custody.

Video court is becoming more popular which means offenders do not have to physically leave the correctional facility. Justice uses a report from CMIS on a daily basis to identify offenders who have video court.

In the past, Justice has released offenders from correctional facilities in error. To reduce these occurrences, as noted above, Justice created the offender return form, developed a spreadsheet to assist with the calculation of a release date when a CSO is violated, and created a sentence management team.

At the completion of sentence management audits, the sentence management team creates summary reports that highlight all errors found. The report for each audit is provided to senior management. At the end of the year, the sentence management team summarizes the results of all audits completed and provides the report to the Deputy Minister. Since the creation of the sentence management team, the number of calculation errors has gone down and the magnitude of the errors has also gone down. However, as noted earlier in Section 5.1, the scope of the sentence management team's work is not based on an approved risk-based plan for auditing offender files and CMIS data. Therefore not all errors for the year may be identified and reported, and senior management may not be aware of the extent of errors in release dates.

6. We recommend that the Ministry of Justice provide senior management with routine reports that completely describe the risk of incorrect offender release dates, how that risk is managed, and all inappropriate offender releases.

As we described earlier, Justice does not know if it is releasing all offenders at the right time. In the event an offender is released from a correctional facility in error, Justice has

an escalation process whereby an unlawful detention-release notification form gets completed and is provided to senior management.

6.0 Selected References

Australian National Audit Office. (2005-06). *Integrity of Electronic Customer Records*. Canberra, Australia: Author.

Australian National Audit Office. (2008-09). *Quality and Integrity of the Department of Veterans' Affairs Income Support Records*. Canberra, Australia: Author.

Canadian Institute of Chartered Accountants and American Institute of Certified Public Accountants. (2009). *Trust Services Principles, Criteria, and Illustrations*. New York: Author.

Canadian International Development Agency. (2005). *Data Integrity Control Framework*. Ottawa: Author.

International Organization for Standardization. (2005). ISO/IEC 27002:2005(E). *Information technology – Code of practice for information security management; 2nd Edition*. Geneva: Author.

Office of the Inspector General. (2004). *Review of the United Marshals Service's Prisoner Tracking System*. Washington, D.C.: Author.

The Information Systems Audit and Control Foundation. (2007). *CoBiT4.1*. Rolling Meadows, IL: Author.