# Section 5

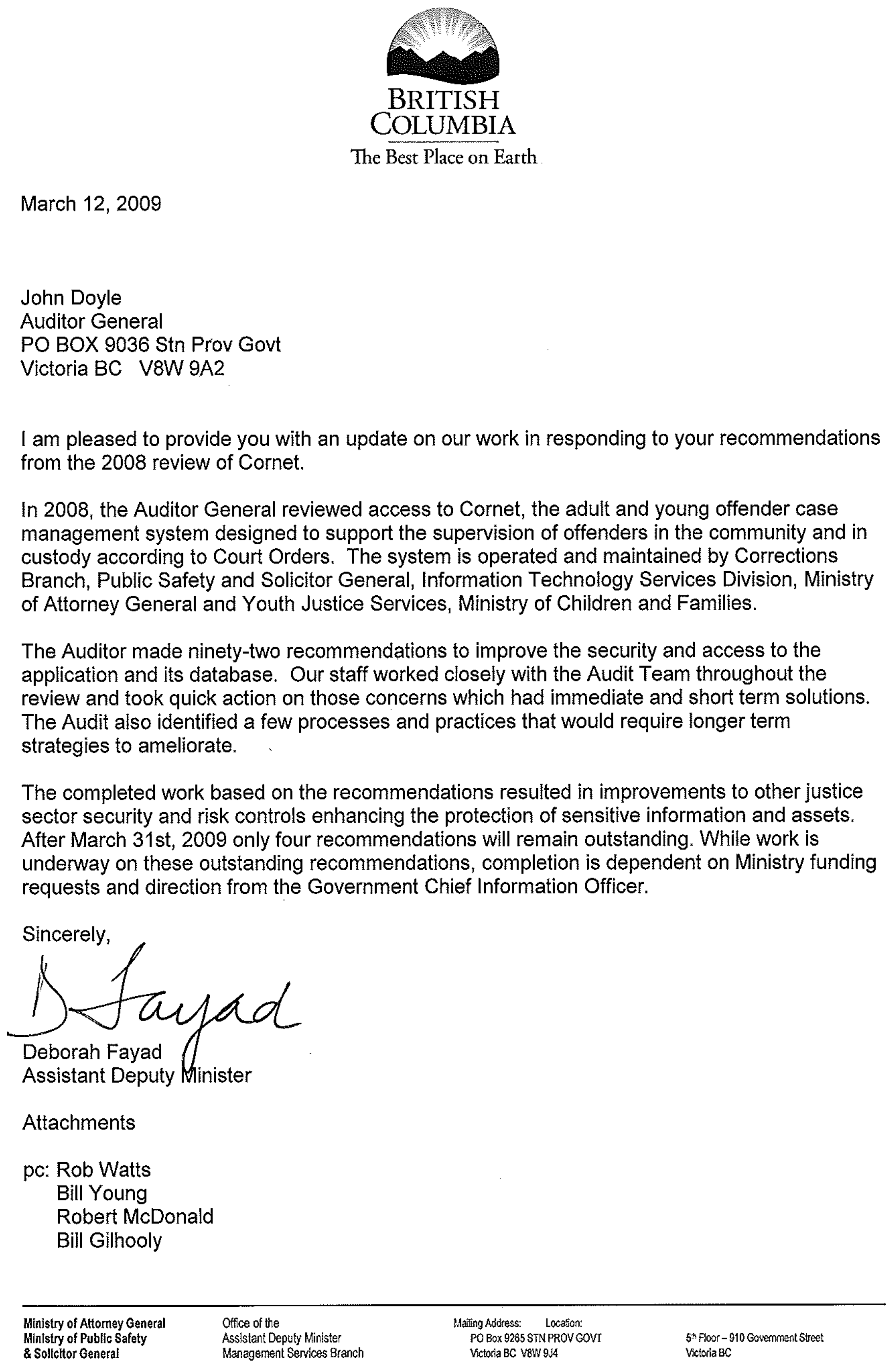
Update on the implementation of recommendations from:

## Managing Access to the Corrections Case Management System

March 2008

April 2009

# Response from the Ministry of Attorney General and the Ministry of Public Safety and Solicitor General



BRITISH
COLUMBIA
The Best Place on Earth

March 12, 2009

John Doyle
Auditor General
PO BOX 9036 Stn Prov Govt
Victoria BC V8W 9A2

I am pleased to provide you with an update on our work in responding to your recommendations from the 2008 review of Cornet.

In 2008, the Auditor General reviewed access to Cornet, the adult and young offender case management system designed to support the supervision of offenders in the community and in custody according to Court Orders. The system is operated and maintained by Corrections Branch, Public Safety and Solicitor General, Information Technology Services Division, Ministry of Attorney General and Youth Justice Services, Ministry of Children and Families.

The Auditor made ninety-two recommendations to improve the security and access to the application and its database. Our staff worked closely with the Audit Team throughout the review and took quick action on those concerns which had immediate and short term solutions. The Audit also identified a few processes and practices that would require longer term strategies to ameliorate.

The completed work based on the recommendations resulted in improvements to other justice sector security and risk controls enhancing the protection of sensitive information and assets. After March 31st, 2009 only four recommendations will remain outstanding. While work is underway on these outstanding recommendations, completion is dependent on Ministry funding requests and direction from the Government Chief Information Officer.

Sincerely,

D Fayad

Deborah Fayad
Assistant Deputy Minister

Attachments

pc: Rob Watts
Bill Young
Robert McDonald
Bill Gilhooly

| | | | |
|---|---|---|---|
| **Ministry of Attorney General**<br>**Ministry of Public Safety**<br>**& Solicitor General** | Office of the<br>Assistant Deputy Minister<br>Management Services Branch | Mailing Address:<br>PO Box 9265 STN PROV GOVT<br>Victoria BC V8W 9J4 | Location:<br>5th Floor – 910 Government Street<br>Victoria BC |

**RECOMMENDATION STATUS SUMMARY**
***Managing Access to the Corrections***
***Case Management System***
**As at January 31, 2009**

| Auditor General's Recommendations | Implementation Status | | | | |
|---|---|---|---|---|---|
| | Fully | Substantially | Partially | Alternative Action | No Action |
| 1. A process should be implemented for promptly informing key staff when user access needs to be modified because an employee's status has changed. | X | | | | |
| 2. Exception reporting and regular monitoring should be conducted to identify and remedy incorrect access. | X | | | | |
| 3. The database access levels should be corrected and regular monitoring conducted to ensure that access remains properly set and that all entries made directly to the database are detected. | X | | | | |
| 4. Strategies, including effective monitoring, should be adopted to address the risk of users having full access. | X | | | | |
| 5. Remove the ability to overwrite the audit trail from all users accessing the database directly. | X | | | | |
| 6. The Oracle userid should be locked and only authorized support staff allowed to access it through their own userids. | X | | | | |
| 7. Firewall settings should be reviewed and any excessive access removed. | X | | | | |
| 8. A patching strategy should be adopted and implemented to address security related vulnerabilities. | X | | | | |
| 9. A strategy should be developed to ensure the adherence of security policies in the implementation of security settings and processes. | | X | | | |

## PROGRESS IN IMPLEMENTING RECOMMENDATIONS FROM

### *Managing Access to the Corrections Case Management System*

### As at January 31, 2009

## General comments

In 2008, the Auditor General reviewed access to Cornet, a comprehensive adult and young offender case management system designed to support the supervision of 27,000 offenders in the community and 3000 offenders in custody according to Court Orders.  The system is operated and maintained by Corrections Branch, Public Safety and Solicitor General, Information Technology Services Division, Ministry of Attorney General and Youth Justice Services, Ministry of Children and Families.

The Auditor made 9 key recommendations to improve the security and access to the application and its database.  Our staff worked closely with the Audit Team throughout the review and took quick action on those concerns which had immediate and short term solutions.  The Audit also identified a few processes and practices that would require longer term strategies to ameliorate.

We are pleased to confirm that after March 31st, 2009, eight key recommendations are fully implemented.  One key recommendation is substantially complete with finalization dependent on Ministry funding requests and central government information technology initiatives.  Additionally, we would like to recognize the Audit and the work undertaken by the Ministry's in addressing the recommendations has resulted in improvements to other justice sector security and risk controls designed to protect sensitive information and assets.

## Progress by recommendation

| Self-Assessed Status | Actions Taken Since Report Issued | Results of Actions and/or Actions Planned (with information on implementation) |
|---|---|---|
| **Recommendation 1:** A process should be implemented for promptly informing key staff when user access needs to be modified because an employee's status has changed. | | |
| F | A process has been implemented between system services and ITSD to promptly inform key staff when an employee's status has changed. | An annual review of the employment status will be conducted.  The process itself will be evaluated and improved as required. |

**Status**

**F** or **S** – Recommendation has been fully or substantially implemented
**P** – Recommendation has been partially implemented
**AA** – Alternative action has been undertaken, general intent of alternative action will addresses OAG  finding
**NA** – No substantial action has be taken to address this recommendation

# Response from the Ministry of Attorney General and the Ministry of Public Safety and Solicitor General

| | | |
|---|---|---|
| **Recommendation 2:** Exception reporting and regular monitoring should be conducted to identify and remedy incorrect access. | | |
| F | A review of access was conducted and problems remediated. | Periodic exception reporting and regular monitoring are in place. |
| **Recommendation 3:** The database access levels should be corrected and regular monitoring conducted to ensure that access remains properly set and that all entries made directly to the database are detected. | | |
| F | A review of database access levels was conducted and problems remediated. Logging of access entries to the database was extended. | Periodic reviews are in place to verify appropriate database access levels. |
| **Recommendation 4:** Strategies, including effective monitoring, should be adopted to address the risk of users having full access. | | |
| F | There is a strategy in place for monitoring and review of users with full access. | Periodic reporting and regular monitoring are in place. |
| **Recommendation 5:** Remove the ability to overwrite the audit trail from all users accessing the database directly. | | |
| F | The ability to overwrite audit trails was removed from all users accessing the database directly. | |
| **Recommendation 6:** The Oracle userid should be locked and only authorized support staff allowed to access it through their own userids. | | |
| F | The Oracle userid is locked. Authorized staff use their own userids to access the database. | |
| **Recommendation 7:** Firewall settings should be reviewed and any excessive access removed. | | |
| F | Firewall settings have been reviewed and excessive access removed. | |
| **Recommendation 8:** A patching strategy should be adopted and implemented to address security related vulnerabilities. | | |
| F | A patching strategy was adopted and processes are in place to review and address security related vulnerabilities. | The patching strategy has been initiated and will be evaluated and improved as required. |
| **Recommendation 9**: A strategy should be developed to ensure the adherence of security policies in the implementation of security settings and processes. | | |
| S | A strategy was developed to manage the implementation of security settings and processes for adherence to security policies. | ITSD Security group is increasing its oversight capability of security policies compliance. |

| | |
|---|---|
| **Status** | **F** or **S** – Recommendation has been fully or substantially implemented |
| | **P** – Recommendation has been partially implemented |
| | **AA** – Alternative action has been undertaken, general intent of alternative action will addresses OAG finding |
| | **NA** – No substantial action has be taken to address this recommendation |