BRITISH COLUMBIA

STATEMENT

For Immediate Release
2013JAG0026-000108
Jan. 24, 2013

Ministry of Justice

Ministry tightens JUSTIN network security

VICTORIA – Minister of Justice and Attorney General Shirley Bond has issued the following statement:

“We received the auditor general’s access and security audit on the JUSTIN system and thank him for his recommendations and the additional time he provided us to improve the system that integrates, manages and stores criminal case information from provincial justice agencies.

“Implementing the recommendations is a priority, and I directed Ministry of Justice staff to take immediate action. Already significant security risks in the JUSTIN system have been addressed.

“As a result of the recommendations in Mr. Doyle’s report, information security for B.C.’s justice case-tracking system has been reinforced with stronger defence mechanisms to prevent unauthorized and inappropriate access.

“These changes have been made as a result of the ministry accepting all of the auditor general’s findings in a recent access and security audit on the JUSTIN system.

“Specifically, the ministry has tightened access to sensitive information, enhanced security controls, and put in place new monitoring capabilities. In addition, an action plan and project team are in place to oversee an ongoing project that will address any remaining gaps and will ensure continuous improvement of the security of the JUSTIN system. This will be done in co-operation with the auditor general’s office and we welcome the continued role that the auditor general will have in monitoring our progress.

“Information security is of vital importance in the 21st century. The ministry has every confidence in the JUSTIN system’s security and how it guards against inappropriate access and protects sensitive data from unauthorized eyes.”

Media Contact: James Beresford
Government Communications and Public Engagement
Ministry of Justice
250 387-8119

Connect with the Province of B.C. at: www.gov.bc.ca/connect

BACKGROUNDER

Enhanced JUSTIN security

- System access is now regularly monitored to immediately detect compromised accounts or inappropriate access.
- System administrators must now use a secure access gateway to connect to any high-security justice database. Direct connections from non-government computers are no longer possible. Security has also been heightened with more complex password policies for authorized users.
- Access to JUSTIN for government employees outside of the Ministry of Justice won't be granted unless a valid business need can be proven and appropriate approvals received.
- Training materials and guidelines are being updated to ensure data in the system is properly classified and secured.
- All contractors with access to JUSTIN must undergo a criminal record check. Information technology support contractors also face more enhanced security screening.
- Criminal record checks for employees are under evaluation and changes are underway.
- Permissions have been removed for employees who no longer need to use JUSTIN, or only require limited access, due to a job change or a shift in their responsibilities.
- With the creation of a single Ministry of Justice, the responsibility of the full set of justice applications, including CORNET and JUSTIN, is now under a single chief information officer. Lessons learned from one system will now be applied throughout the rest of the applications. These changes should prevent the gap that resulted in the auditor general's assessment.
- In order to address the issue of user access to Reports to Crown Counsel (RCCs), the following changes have been made:
    - The number of users has been reduced by 800 and monitoring has been put in place for those who have access.
    - Active, sensitive RCCs have been reviewed to ensure access has been applied properly. Work continues with Crown counsel on implementing changes to JUSTIN that refine access privileges on a "need to know" basis.

Media Contact:

James Beresford
Government Communications and Public Engagement
Ministry of Justice
250 387-8119

Connect with the Province of B.C. at: www.gov.bc.ca/connect

CONFIDENTIAL ISSUES NOTE Ministries: Justice, Citizens’ Service & Open Government Date: Updated Jan. 23, 2013 Minister Responsible: Shirley Bond	**Auditor General report: JUSTIN (Justice Information) System**

ADVICE AND RECOMMENDED RESPONSE:

- **We have accepted all of the Auditor General's findings and assigned a project team to address the report’s recommendations.**
- **Good progress has been made with several actions already completed or well underway to resolving the issues identified by the auditors.**
- **I would like to thank the Auditor General and his staff for their work on the JUSTIN access and security audit.**
- **The recommendations have guided important changes to the system that will help ensure it remains free of any privacy or security breaches.**
- **We appreciate the extra time the Auditor General granted us to respond and implement the majority of the report’s recommendations before they were publicly released.**

<u>If asked, about Ministry response to recommendations</u>

- **We have implemented several new policies and taken corrective actions to address the Auditor General’s recommendations to improve JUSTIN’s security.**
- **JUSTIN access has been reviewed and users who no longer require access have had their permissions removed.**
- **Other actions include more stringent monitoring, more complex password requirements, and proof of a valid business need to gain any network access from other ministries.**

- **Additional steps involve updated training materials, enhanced security screening for contractors, restricting access to sensitive files, and removal of permissions no longer needed by former employees.**
- **More work will be done in the coming months to make JUSTIN even more secure.**

<u>If asked, about what else is planned (including RCCs)</u>

- **Controls will be set so that users only have access to system areas or functions that are relevant to their roles and positions.**
- **JUSTIN will be moved and housed in a new data centre, monitoring and auditing capabilities will be further improved, and information technology (IT) infrastructure will be enhanced.**

KEY FACTS REGARDING THE ISSUE:

- The Auditor General will release his report “Securing the JUSTIN System: Access and Security Audit at the Ministry of Justice” on January 24, 2013.
- The report was originally scheduled for release on December 6, 2012. However at the request of the Attorney General, the release was deferred to give the ministry more time to respond to the report’s findings and recommendations.

<u>Audit Conclusions:</u>

- The auditor general’s report reaches two main conclusions:
  1. Information in the JUSTIN system is inadequately protected from internal or external threats; and
  2. Controls in the JUSTIN system are inadequate to detect or prevent unauthorized access.

<u>Audit Recommendations:</u>

- The auditor general’s report makes five key recommendations:
  1. Multiple layers of security need to be in place. Controls in network and system components should be reviewed, reconfigured, documented and better managed.
  2. User access should be granted and managed based on the “need to know” principle.

3. Highly sensitive JUSTIN information should be properly classified and secured with extensive monitoring.
4. More effective audit trails and tools to detect and investigate suspicious or unauthorized activity.
5. An effective monitoring program to proactively detect unauthorized access and removal of copied JUSTIN information.

- Ministry of Justice has already taken several steps to address the recommendations presented in the audit report.
- In addition to the immediate mitigations, work is being done to deal with the longer term concerns identified.

Immediate Actions Taken:

- System access is now regularly monitored to immediately detect compromised accounts or inappropriate access.
- System administrators must now use a secure access gateway to connect to any high-security justice database. Direct connections from non-government computers are no longer possible. Security has also been heightened with more complex password policies for authorized users.
- Access to JUSTIN for government employees outside of the Ministry of Justice won't be granted unless a valid business need can be proven and appropriate approvals received.
- Training materials and guidelines have been updated to ensure data in the system is properly classified and secured.
- All contractors with access to JUSTIN must undergo criminal records checks. Information technology support contractors for the system also face more intense security screening.
- Permissions have been removed or reduced for employees who no longer need to use JUSTIN, or only require limited access, due to a job change or a shift in their responsibilities.

Next Steps Planned:

- Establishing more granular access for Reports to Crown Counsel (RCCs).
- A move to a new data centre will house JUSTIN in a more secure, state-of-the-art computing facility with improved safeguards and better segregation between systems and environments.
- A new, enhanced security function in the ministry's Information Systems Branch will improve system monitoring and auditing capabilities.

- Ministry information technology (IT) staff are working closely with central government IT to improve security of shared infrastructure services.

Media Coverage:

-

Not Responsive

This document may contain information that is protected by solicitor client privilege. Prior to any disclosure of this document outside of government, including in response to a request under the <u>Freedom of Information and Protection of Privacy Act</u>, the Ministry in possession of this document must consult with the lawyer responsible for the matter to determine whether information contained in this document is subject to solicitor client privilege.

Communications Contact:	Cory Shirshac/Heather Smart (778-679-8203)
Program Area Contact:	Bobbi Sadler (387-5910)/ Joyce DeWitt-Van Oosten (250-387-5174)
File Created:	
File Updated:	Jan. 23, 2013
File Location:	

Minister's Office	Program Area	Deputy	Comm. Dir
To MO XX			L. Mulholland Jan 9 C. Heiman

JUSTIN is a computerized system used by B.C. to manage and administer the criminal justice process. It allows adult and youth criminal cases to be tracked and processed from initial police arrests and Crown counsel charge assessments through to court judgments.

Questions and Answers
Auditor General Access and Security Audit on the Justice Information (JUSTIN) System
January 2013

1. **What have you done to address the Auditor General's recommendations?**
   - System access is now regularly monitored to immediately detect compromised accounts or inappropriate access.
   - System administrators must now use a secure access gateway to connect to any high-security justice database. Direct connections from non-government computers are no longer possible. Security has also been heightened with more complex password policies for authorized users.
   - Access to JUSTIN for government employees outside of the Ministry of Justice won't be granted unless a valid business need can be proven and appropriate approvals received.
   - Training materials and guidelines have been updated to ensure data in the system is properly classified and secured.
   - All contractors with access to JUSTIN must undergo criminal records checks. Information technology support contractors for the system also face enhanced security screening.
   - Permissions have been removed or reduced for employees who no longer need to use JUSTIN, or only require limited access, due to job change or shift in their responsibilities.
   - We have addressed or are addressing all of the findings highlighted in the report. However, at this time, we are only able to mitigate the risks relating to printing through educating users and reiterating security and privacy policies. We continue to explore technological solutions to address this finding.

<u>If asked about specific recommendations:</u>

1. Controls in network and system components in the JUSTIN environment should be reviewed, reconfigured, documented and better managed to ensure multiple security layers are in place.

- All remote accounts have been reviewed and users who no longer require access have been removed.
- Network access has been reviewed and modified to remove access to the Justice systems by employees in other ministries unless a valid business need can be proven (e.g. MCFD Youth Justice).
- Process is in place to continually log and monitor network traffic to ensure inappropriate access to the network is being detected.

2. User access to JUSTIN information should be granted and managed based on the principle of 'need to know'.

- We have reduced the number of users by 800 and will monitor those with access.
- Active sensitive RCCs have been reviewed to ensure access has been applied properly. A review of historical data is being analyzed for future inclusion as part of the ongoing review of the JUSTIN access model.
- We will continue to work with Crown counsel on implementing changes to JUSTIN that refine access privileges on a "need to know" basis.
- Helpdesk staff are receiving Human Resource lists and making necessary changes to staff access and authority levels

3. Highly sensitive JUSTIN information should be properly classified and secured with extensive monitoring in place.

- Work on this is underway and already we have classified access to all active reports by crown counsel. As part of justice reform initiatives we have committed to moving towards Crown file ownership and that will enable further improvements in this area.
- Training materials and guidelines are being updated to ensure staff and partners are properly classifying and security data within the system.
- Further enhancements to monitor user activity will be introduced by additional system monitoring and auditing capabilities, thereby greatly enhancing our ability to detect inappropriate system usage or activity.

4. More effective audit trails and tools should be in place to enable detection and investigation of suspicious or unauthorized activity.

- We are now logging and monitoring the activity of JUSTIN users to detect compromised accounts
- Additional system tools and software will be implemented to ensure detection and unauthorized activity is detected.
- Over the coming months, the ministry will move its applications to new data centres which will ensure that JUSTIN is housed in a secure, state-of-the-art computer facility, with improved safeguards and better segregation between systems and environments.

5. An effective monitoring program should be in place to enable proactive detection of unauthorized access and removal of copied JUSTIN information.

- System administrators must now use a secure access gateway to connect to any high-security justice database. Direct connections from non-government computers are no longer possible. Security has also been heightened with more complex password policies for authorized users, and all access is logged and monitored.
- Alerts if an unrecognized user tries to log on with incorrect credentials.

2. More work needs to be done to make JUSTIN security even better. What else is planned?

- Establishing a role-based security model for the JUSTIN
- A move to a new data centre will house JUSTIN in a more secure, state-of-the-art computing facility with improved safeguards and better segregation between systems and environments.
- A new, enhanced security function in the ministry's Information Systems Branch will improve system monitoring and auditing capabilities.
- Ministry information technology (IT) staff are working closely with central government IT to improve security of shared infrastructure services.
- The Ministry will also continue to meet regularly with the Auditor General team to ensure an optimal understanding of the report's findings and the additional remediation work that still needs to be done.

3. What is the timeline or timeframe for addressing the remaining gaps?

We have a plan in place that will close remaining gaps over the next 12 months.
Some activities will be complete much sooner than that, but moving JUSTIN and all its related infrastructure to a new secure data centre is the culmination of a great deal of ongoing work to align to government's new strategic direction for information systems hosting. This work was well underway prior to the audit report.

4. Is the JUSTIN system adequately protected from security threats and attacks?

Yes, the auditor general's own findings indicate JUSTIN is protected from external attacks initiated from the Internet. Furthermore, JUSTIN is also secure from direct attack from the government's own network in the event that an individual should gain unauthorized access to the government network through another ministry.

The report indicated that we had gaps in the amount of access we were granting to individuals and how this access was being monitored. We have now put in place controls to mitigate gaps indicated by the report.

A lot of work was done in a relatively short period of time to address the audit's findings. This work was done in consultation with Auditor General staff by a project team of ministry staff and contractors, reps from RCMP and municipal police, and our partners in the Ministry of Citizen Services (who provide IT services to all ministries) as well as their contracted service providers.

5. What is the likelihood of JUSTIN being penetrated by an internal threat or an external attack? Has any kind of threat assessment been done?

A threat and risk assessment was performed. Based on that assessment we developed and implemented a plan that adds new security controls to address the identified vulnerabilities.

But no matter how much we reduce the risk, or how unlikely a security breach, there is no such thing as zero risk. This is why we have developed an ongoing plan that will continue to improve security and further reduce risk from security threats – not just for JUSTIN, but for all our justice applications.

I should also point out that the Ministry advised the Auditor General that some of the information contained in this report could invite curious hackers to try and penetrate the system, creating an additional security risk.

However, the release of this information is entirely at the discretion of the Auditor General. The ministry provided the conclusions from the threat risk assessment to ensure the Auditor General was fully informed in his decision to publicly release this information.

6. Are controls in the JUSTIN system adequate to detect unauthorized access?

Yes, access to the JUSTIN application is logged and JUSTIN now has additional monitoring controls in place that provide us with the ability to detect unauthorized users.

The Ministry of Justice will continue to enhance this security monitoring function with additional monitoring capabilities and auditing to better monitor the activities of authorized users.

7. Why didn't you make these improvements on your own? Why did it take an audit to spur you into action?

Many of the recommendations in this audit are things that we ourselves communicated to the auditors as needing to be improved upon. Many of these improvements are things that were already being addressed by existing initiatives.

Not Responsive

Not Responsive

Not Responsive

JUSTIN IN GENERAL

9. Has the JUSTIN system ever been previously compromised?

As technology has changed the ministry has made a firm commitment to ensure that its information systems keep pace to remain as secure as possible.

To the best of our understanding, we have never had any hacker or external attacker compromise the JUSTIN system itself.

When we have had incidents where JUSTIN information was disclosed inappropriately, the Ministry Response Plan ensured all safety and security concerns were addressed right away, including notifying the persons who were potentially impacted and involving police if required. Appropriate actions to ensure public safety and the integrity of the justice system were implemented in all cases.

10. How many people had access to JUSTIN before the audit was conducted? How many now have access?

Before the audit 3,300 people had access to JUSTIN Reports to Crown Counsel (RCCs). As of today, we have reduced that number to under 2,500.

11. Didn't JUSTIN have previous problems with an error in processes for automated "intrusion alerts" as well as firewall settings related to virtual private network accounts?

These were issues that were detected early in the process of this current audit. They were addressed immediately upon notification to ministry staff by the auditors.

12. Who manages and uses JUSTIN?

Not Responsive

There are nearly 2,500 JUSTIN users with access to Reports to Crown Counsel.

Not Responsive

Not Responsive

Not Responsive

AUDIT REPORT

14. What are the audit's two main conclusions?

- Information in the JUSTIN system is inadequately protected from internal and external threats.
- Controls in the JUSTIN system are inadequate to detect or prevent unauthorized access.

15. What are the audit's five overarching recommendations?

- Multiple layers of security need to be in place. Controls in network and system components should be reviewed, reconfigured, documented and better managed.
- User access should be granted and managed based on the "need to know" principle.
- Highly sensitive JUSTIN information should be properly classified and secured with extensive monitoring.
- More effective audit trails and tools to detect and investigate suspicious or unauthorized activity.
- An effective monitoring program to proactively detect unauthorized access and removal of copied JUSTIN information.
- Underlying these five general suggestions are 100 detailed recommendations to address cited problems.

Not Responsive