Securing the JUSTIN System: Access and Security Audit at the Ministry of Justice

As at: August 9, 2013
Released: 24 Jan 2013
Discussed by the Public Accounts Committee: N/A

Self-assessment conducted by Information Systems Branch, Ministry of Justice

Comments

"The Ministry of Justice continues to make significant efforts to address all of the recommendations in this audit report. The first phase of the audit response focused on two primary activities. First, it involved completing any recommendation where an immediate solution existed . Second, it mitigated the risks associated with audit findings where the recommendations were complex or required a long-term solution.

Significant progress has been made but the remaining work involves many of the more complex recommendations. Even though the ministry is dedicating considerable resources towards implementing these recommendations, this work will take time to complete.

The remaining recommendations are being treated in a more comprehensive manner. The ministry is undertaking an initiative to address the specific audit recommendations while simultaneously enhancing the overall effectiveness and capabilities of its information security functions. This approach goes beyond the audit recommendations in many areas. Although it is more time consuming, this will help ensure that JUSTIN information remains secure on an ongoing basis and that other systems also benefit from the changes being made for JUSTIN.

The specific details of the work completed for each of the five recommendations are outlined below.

Please note that the five high-level recommendations contained in the audit report summarize 100 detailed audit recommendations made by the Auditor General as well as the additional work the ministry is undertaking that goes beyond the audit recommendations. While ongoing work in each of these areas remains in progress, many of the specific recommendations have been fully completed. Ministry staff meet regularly with staff at the Office of the Auditor General to provide status updates on each of these detailed recommendations. The ministry's self assessed status of "Partially implemented" reflects the fact that there is a mixture of completed, partially completed and outstanding recommendations in each of these five areas."

Recommendations

RECOMMENDATION AND SUMMARY OF PROGRESS	SELF-ASSESSED STATUS
Recommendation 1: Controls in network and system components in the JUSTIN environment should be reviewed, reconfigured, documented and better managed to ensure multiple layers of security are in place.	**Partially implemented**

Actions taken, results and/or actions planned

"The ministry has reviewed network controls and system components and has taken steps to ensure that multiple levels of security are in place. Immediate changes were made where possible. In order to fulfill the remainder of the recommendations related to the security of the system components, the JUSTIN system will be moved from its current infrastructure to an entirely new data centre. All the physical system components including the servers and network infrastructure will be entirely new.

Complete: Network access has been reviewed and modified to remove access to any Justice systems by employees in other ministries unless a valid business need can be proven and approvals have been given. Remote accounts issued to regular government users are no longer able to access JUSTIN or other sensitive applications within the Ministry of Justice environment. All unnecessary connections to the JUSTIN database have been eliminated.

System administrators are now required to use a "Secure Access Gateway" to connect to any high-security Justice databases, including the JUSTIN database. There are no longer any direct connections from non-government computers and password policies have been updated for privileged operating system accounts.

Criminal records checks are now required for all new employees who will have access to JUSTIN and contractors and staff with privileged administrator access to the system must now submit to enhanced security screening.

In Progress: A move to new data centres is underway which will ensure that the JUSTIN system is housed in a secure, state-of-the-art computing facility, with improved safeguards and better segregation between all ministry applications including JUSTIN. This migration requires careful planning and coordination with other stakeholders as JUSTIN contains multiple modules and many of these modules integrate with external systems. Work is scheduled to complete by April 2014.

Planned: Vulnerability scanning will be carried out for all of the ministry's most sensitive applications such as JUSTIN. This scanning will provide assurances that JUSTIN remains secure once it is migrated to the new data centre."

Recommendations (Continued)

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

Actions taken, results and/or actions planned

"The ministry took immediate steps to remove any user that did not have a current need for access to the system. Security around sensitive files was reviewed and some groups of users had their access reduced. For a more permanent and complete solution the ministry is reviewing the current access model and will undertake system changes to allow JUSTIN access to be controlled in a way that permits users to only have access to the information they need to do their jobs. The access model currently built into the system does not allow for this level of access control.

Complete: JUSTIN access has been reviewed and users who no longer require access have had their permissions removed. We have ensured that the security features in JUSTIN that should restrict access are applied properly to all active sensitive RCCs. Staff changes are carefully monitored and access to JUSTIN is removed immediately when an employee changes jobs or no longer requires access.

In Progress: A working group representing all of the major JUSTIN stakeholders was tasked with determining need-to-know requirements for the RCC data for each user role in JUSTIN. The group has developed a draft model of JUSTIN information access requirements. This is being analyzed to determine the gaps between the required access controls and what is possible with JUSTIN's current application software. The final result will be a new security access matrix. This work is scheduled to complete by November 2013.

Planned: Based on the findings of the working group the ministry will determine which additional security access controls can be incorporated into the existing system and will implement these changes by rewriting parts of JUSTIN's software. It may not be feasible to make all changes within the existing system so the ministry will be using a risk to cost analysis to determine which changes to make. If any new security access controls cannot be added to the existing system, these will be documented and maintained for future consideration.

Maintaining JUSTIN user access lists still involves many manual steps. Future enhancements to user access management are planned to help automate the process which will make it more efficient and less vulnerable to human error. The scope of this will extend beyond JUSTIN to many of the ministry's systems."

Recommendation 3: Highly sensitive JUSTIN information should be properly classified and secured with extensive monitoring in place. **Partially implemented**

Actions taken, results and/or actions planned

"The ministry has ensured that all users are aware of current system controls for securing information within JUSTIN. Changes to JUSTIN and a new monitoring program, described under recommendations two and five respectively, will enable us to fully complete this recommendation.

Complete: Training materials and guidelines have been updated to ensure that staff and partners are aware of JUSTIN's existing security features and are properly securing data within the system.

Planned: Pending the completion of work to design JUSTIN's new security access model, the ministry will carry out further updates to business processes and JUSTIN usage policies. Additional classification of information and monitoring of access are included in this scope.

Further details of monitoring enhancements are provided under recommendation five below."

Recommendations (Continued)

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

Actions taken, results and/or actions planned

"Maintaining JUSTIN's user access lists still involves many manual steps. Future enhancements to user access management are planned to help automate the process which will make it more efficient and less vulnerable to human error. The scope of this will extend beyond JUSTIN to many of the ministry's systems.

Audit trails have been added to the system which now allow for the detection of unauthorized users. New tools are being introduced that will allow for enhanced detection of suspicious activity and easier auditing of inappropriate user access.

Complete: JUSTIN system access is now being monitored to detect compromised accounts: this enhances our ability to detect anomalous system usage that could be could be indicative of inappropriate access.

In Progress: New audit tool software has been acquired and is currently being deployed. This software not only provides additional audit trails regarding access to the JUSTIN database, it also makes it much easier to interpret this information and can provide automated security alerts of suspicious activity. The audit tool will be applied to JUSTIN as well as several other sensitive ministry databases.

The audit tool is scheduled to be in place by December 2013.

Planned: Additional audit capabilities will be developed as part of the enhanced information security program that ministry is undertaking. Details are provided under recommendation five below."

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

Actions taken, results and/or actions planned

"In response to this audit the ministry is enhancing its overall information security capabilities. Initial steps to implement improved system monitoring have been completed. A new security program is being implemented and will feature an enhanced monitoring function that will significantly increase our capacity to monitoring for unauthorized and inappropriate access.

Complete: Unauthorized external connections and inappropriate access to data from operating system accounts is now being monitored on the JUSTIN database.

In Progress: A new information security program is being developed which will incorporate existing information security staff into an enlarged group under a new director of information security. The ministry is currently running a competition to fill the new director position. The position is expected to be filled by September 2013.

Planned: After the director is in place, the next information security position to be filled will be a security analyst responsible for security auditing and monitoring. This role will oversee the operation of the audit tool described under recommendation four as well as be responsible for additional monitoring of JUSTIN and its infrastructure.

Beyond the audit recommendations but as part of this enhanced security initiative the ministry is exploring options to deploy a Security Information Event Management solution. This solution will allow security log information to be correlated from multiple sources, thereby enhancing our ability to detect unauthorized access."