BRITISH TRANSPORT POLICE

Report to:	**Audit & Risk Assurance Committee**
Agenda item:	**7**
Date:	**6 September 2016**
Subject:	**Op Canberra**
Sponsor:	**Simon Downey**
For:	**Information**

1. PURPOSE OF PAPER

1.1 The purpose of this report is to update the Committee following the closure of Operation Canberra which dealt with legacy information management issues.

2. BACKGROUND

2.1 The Information Management Unit was formed in 2013 following a review of information management across the force, which recommended a centralized department that should report to one Chief Officer lead. Throughout 2013 a strategy and plans were put in place to deal with many legacy problems with both physical and electronic police records. Work had commenced within the Crime Directorate to improve intelligence processes and a Chief Inspector within Information Management had been appointed to establish a team to recall and review 10,000 unindexed boxes stored in Iron Mountain.

2.2 In January 2014 the Chief Constable was asked to attend a Home Affairs Select Committee Meeting to provide a response to questions posed by the chair about legacy information management issues. Accordingly, a Police Operation commenced in order to expedite remedial work. The work was in two strands; physical records stored initially in Iron Mountain that were unindexed and electronic intelligence records that were not linked appropriately to person records.

2.3 Physical records were recalled from Iron Mountain and were then subject to a retention, review and disposal process at Caledonian Road police station by a mixture of police officers, temporary staff and subject experts.

2.4 The electronic records and specifically intelligence reports held on the old Force Intelligence System (FIS) were subject to a similar process as the physical records albeit the focus was specifically to identify those records which required uploading to the Police National Database (PND). PND is the national police database which enables and highlights information being held by a force against an individual.

2.5 Both the issue with the physical records and the electronic records posed significant risk to the force through failure to comply with Data Protection Legislation and through lost investigative opportunities through the unavailability (no ease of access) of both physical and electronic records.

3. ACTIONS

3.1 The Operation identified all the third party suppliers of archiving services to the force and recalled the material from each of them, as well as then addressing locally held records and reviewing indexed boxes stored at Iron Mountain. This led to the recovery in total of over 39,000 boxes of material and the complete review of this material to determine its correct classification under the three MOPI headings i.e. those papers that need retaining for up to 6 yrs. - MOPI 3, up to 10 years – MOPI 2 and those for up to 100 years for MOPI 1. Following a review of the material 7395 boxes of sorted data was submitted to Iron Mountain for ongoing retention. As of 30th August 2016, 9344 boxes of material are currently held. All other contracts with third party suppliers have been closed down. The exercise produced over 300 tonnes of confidential waste.

Risk – the Force is now compliant with the principles of the DPA and all archived physical records are now reviewed, weeded where appropriate and correctly referenced and stored at our single storage provider.

3.2 The operation identified that there was a need to invest training and up skilling of all station administrators who have responsibility for placing onto the force archiving system undetected and detected files. This gap has now been closed and over 200 staff were trained to use the force archiving system, CycMoPA. In addition an ongoing user group and resource centers have been created under Information Management's direction to help assist the staff who manage this task. In addition significant work was undertaken to join Niche and CycMoPA to enable the systems to 'Talk' to one another to help the population of data fields on CycMoPA from material held on Niche to drive up data standards and to aid the correct MOPI classification.

Risk – the Force has now put in place training, revised processes and procedures and appropriate audits to ensure the correct archiving of all physical records, thereby complying with the DPA.

3.3 In relation to the review of the 898,000 intelligence records these were prioritized and actioned in the order of severity. The operation identified all the intelligence records that were linked to a MOPI 1, 2 or 3 offenders initially and then sought to determine whether they were linked to an address, vehicle of event (POLE) data. All intelligence reports have now been linked to an offender record and so all remedial actions in relation to intelligence records are complete. The new integrated system, Niche, has been implemented and a small data quality team based in Information Management checks that all events are linked to a golden nominal record.

Risk – the risk is now significantly reduced as Niche works on the basis that all events are linked to a person record. Processes and procedures are in place to ensure clear direction. The data quality team check on a daily basis to ensure those processes are being followed.

3.4 The force archiving system, CycMoPA has also been reviewed as part of the operation. Additional fields have been added and where opportunities existed to improve data recording these have been made. The system has also been reviewed to remove the footprint of deleted records and to date over 200,000 records have been deleted. Work continues to align the retained physical files and the electronic records on CycMoPA and this is overseen by the Force records manager.

Risk – the improvements made reduce the risk of material being inappropriately recorded which will in turn lead to ease of identification and retrieval.

4. COSTS

4.1 The total costs from the commencement of Operation Canberra to August 2016 are £1.53million. This includes all the staff, supplier and additional estate costs due to the need to retain Caledonian Road for a further period of time to complete the exercise.

5. IRON MOUNTAIN

5.1 This company supplies all the forces ongoing archived services. Supplier meetings were held at regular meetings during the operation to quantify the volume of undrawn boxes and to keep control of security. These meetings have continued since the closure of Op Canberra and are now undertaken by staff within the Information Management team. Monthly Management Information is provided by the supplier to the force detailing volume of boxes held, space occupied and costs incurred. All activity to withdraw boxes is centrally controlled and managed by the Information Management Team. All invoices and activity are subject to central scrutiny. Recall of boxes to be reviewed in the future will also be managed centrally from 2017 (when the next batch are due to be reviewed).

Risk – the risk of boxes not being managed correctly has been significantly reduced through central control and management of this single service provider by the Information Management Team,

6. INFORMATION COMMISSIONER'S OFFICE

6.1 Regular engagement has taken place with the Information Commissioner's Office (ICO) to provide assurance to the ICO on our activity and to ensure all our activity is in line with best practice. Six monthly meetings are in place between the Director of Capability & Resources and the Head of Information Management and Senior Policy Officers in the ICO's Strategic Liaison Office. The ICO stated early in 2016 that they were satisfied that British Transport Police have addressed the problem of records management and they continue to monitor and review our practices.

6.2 In April 2016 BTP instigated a voluntary Information Risk Review which is carried out by the ICO, in order to ensure all revised strategy, policy and processes in this area were fit for purpose. Significantly the review made recommendations for activity that was already underway but had not yet been completed. This provided further reassurance that our strategy and direction was fit for purpose.

6.3 In July 2016 a Government Internal Audit of Information Management took place and the final report is due in early September. The audit is expected to show a high level of assurance in the function of the Information Management Unit and their supporting strategy, policy and procedures, with further work to do to ensure all the work is embedded throughout all departments and divisions.

7. POLICE NATIONAL DATABASE

7.1 Now Niche is implemented we are working on the automatic extraction of our data to upload to the PND. We are working with the Home Office to progress this extract and are on target to resume upload by late September 2016.

Risk - the future ongoing risk regarding nominal upload will therefore diminish once the Home Office confirm that they are ready to receive our data, which is now in an appropriate integrated system based on the golden nominal principle.

8. CONCLUSION

8.1 The risks posed to the Force of non-compliance with the DPA for both physical and electronic police records is considered to be significantly reduced. The contents of the report are submitted to the committee for noting.