



BRITISH TRANSPORT POLICE

19 – 22 MAY 2008

POLICE NATIONAL COMPUTER

COMPLIANCE REPORT

Report Contents

1. EXECUTIVE SUMMARY	2
1.1 INTRODUCTION	2
1.2 BACKGROUND	2
1.3 METHODOLOGY	3
1.5 CONCLUSIONS	5
2. DETAILED FINDINGS AND RECOMMENDATIONS	6
2.1 LEADERSHIP.....	6
2.2 POLICY AND STRATEGY	7
2.2.2 PNC Policy and Strategy	7
2.2.4 Data Protection.....	9
2.3 PEOPLE	10
2.3.1 PNC Awareness	10
2.3.2 Training	10
2.4 PARTNERSHIPS AND RESOURCES.....	11
2.5 PROCESSES.....	12
2.6 RESULTS	14
APPENDIX A	15
Summary of Recommendations for British Transport Police	15
APPENDIX B	16
Summary of Good Practice at British Transport Police.....	16
APPENDIX C	17
Thematic Inspection Report on Police Crime Recording, the Police National Computer and Phoenix Intelligence System Data Quality - 'On The Record'	17
APPENDIX D	19
PRG Report "Phoenix Data Quality" Recommendations	19
APPENDIX E	21
Police National Computer Data Quality and Timeliness – 1 st Report.....	21
APPENDIX F.....	23
Police National Computer Data Quality and Timeliness – 2 nd Report	23

1. Executive Summary

1.1 Introduction

- 1.1.1 Her Majesty's Inspector of Constabulary (HMIC) conducted a Police National Computer (PNC) Compliance Inspection of the British Transport Police between 19th and 22nd May 2008.
- 1.1.2 This report is based on views and comments obtained from strategic, PNC and customer level management and users at Force Headquarters and operational police officers and staff. These views have been supported by reality checks conducted by HMIC PNC Compliance Auditors (known throughout this report as HMIC Auditors).
- 1.1.3 Her Majesty's Inspector would like to place on record his thanks to all members of staff who contributed to this report and provided assistance during the inspection.

1.2 Background

- 1.2.1 The British Transport Police (BTP) are the national police force for the railways throughout England, Scotland, and Wales. The force is also responsible for policing the London Underground, Eurostar, the Channel Tunnel Rail Link, the Docklands Light Railway, the Croydon Tramlink, the Glasgow Subway and the Midland Metro tram system. The force deals with all crimes from murder (subject to agreement with the local police force), to fare evasion and drunkenness, and a host of other incidents including all rail accidents, fatalities, and suicides. While BTP does not police a resident population, it is charged with the safety of some 5 million passengers daily and over 100,000 railway staff.
- 1.2.2 The force has a total of seven territorial basic command units. The headquarters (HQ) of the force is in London and houses the Association of Chief Police Officers team, comprising the Chief Constable, the deputy chief constable, four assistant chief constables and a director of human resources. With 2,770 police officers supported by 250 special constables, 210 police community support officers and 1200 police staff the force faces a significant challenge in policing a diverse and extensive network.
- 1.2.3 The PNC Bureau (PNCB) based at the force HQ operates Monday to Friday from 0800 until 16.00. The duties of the PNCB include the creation of wanted and missing person reports, and a host of other functions to manage the accuracy of PNC reports owned by the force. The PNCB also provides a PNC enquiry service for operational officers including VODS (vehicle online descriptive search) and QUEST (queries using enhanced search techniques) searches. Out of hours the Management of Information and Communications Centre (MICC) will enter the urgent PNC updates such as detained and wanted/missing reports. BTP has an arrangement with Lancashire Constabulary to provide VODS and QUEST searches when the PNCB is closed.

1.2.4 The creation of an arrest summons (A/S) report in BTP is carried out by the Crime Recording Centre (CRC). The police officer telephones for an A/S number giving the CRC operator brief details of the offender; a partial record is created on the PNC at that time. The CRC will then create an electronic source input document on the POINTS (Police Operational Information aNd Tasking System)¹ application for the officer to complete within 24 hours.

1.2.5 Court results are input onto the PNC by criminal justice units based on the BCUs in London, Birmingham, Liverpool Newcastle and Glasgow. Due to the countrywide location of BTP offenders the force has had to make numerous local agreements with the courts in order to receive court results. Bail conditions are also entered when the details are faxed through from the courts.

1.3 Methodology

1.3.1 A full inspection against the 2005 PNC Protocols was carried out covering the sections of Leadership; Policy & Strategy; People; Partnerships & Resources; Processes and Results.

1.3.2 The inspection was conducted over three stages with a final assessment being provided in line with the HMIC Baseline Assessment grading structure of:

- **Excellent** Comprehensive evidence of effective activity against all protocol areas.
- **Good** Evidence of effective activity covering many areas, but not comprehensive.
- **Fair** Evidence of effective activity covering some areas, but concerns in others.
- **Poor** No or limited evidence of effective activity against all the protocol areas; or serious concerns in one or more area of activity.

1.3.3 The first stage of the inspection involved the force providing HMIC Auditors with documentation to support their adherence to the protocols. This was followed up by a visit to the force with HMIC Auditors conducting interviews with key staff. The visit to the Force also incorporated the final stage of the inspection, which was based upon reality checks. The reality checks included a review of PNC data against source documentation (arrest data) and quality checks of the originator line to assess compliance with national policies.

1.3.4 Using the evidence gathered during each stage of the inspection, this report has been produced based upon the European Foundation of Quality Management (EFQM) format.

¹ Every BTP office has a POINTS account which is fed by information from the BTP Crime, Intelligence and e-SID systems. This allows officers to manage their workloads, and additionally allows supervisors to view the progress of any work their officers are involved in.

1.4 Current Performance

1.4.1 On 27th April 2000, ACPO Council endorsed the ACPO PNC Compliance Strategy. The strategy is based upon the following four aspects of data handling:

- Accuracy
- Timeliness
- Completeness
- Relevancy

1.4.2 The strategy is owned by ACPO but is also reliant on other partners taking responsibility for key actions within the strategy. The partners include NPIA (National Police Improvement Agency), HMIC, and individual police forces.

1.4.3 On 1st January 2005, the performance indicators of the ACPO Compliance Strategy were replaced by the timeliness standards contained within the newly published Code of Practice for the PNC. The PNC Code of Practice, developed by the National Centre for Policing Excellence and endorsed by ACPO, is a statutory code made under s.39a of the Police Act 1996 (inserted by section 2 of the Police Reform Act 2002). It provides scope for the Home Secretary to invoke statutory intervention for forces failing to comply. With regards to individual forces, a number of performance indicators (PIs) specifically for PNC data standards were set. Each force has a responsibility to achieve the standards set within the Code of Practice. The timeliness standards within the Code are as follows:

- 90% of recordable offences entered onto PNC within 24 hours of the commencement of proceedings. The commencement of proceedings being defined as when a person is arrested, reported or summonsed.
- From the 1st July 2005, the target is for 75% of all finalisations being entered onto PNC within 7 days of the information being received by the police. For the previous 6 months the target was for 50% of the court results to be entered within 7 days. Courts have their own target of 3 days for delivery of data to the police. Therefore, the police are measured against an overall target of 10 days.

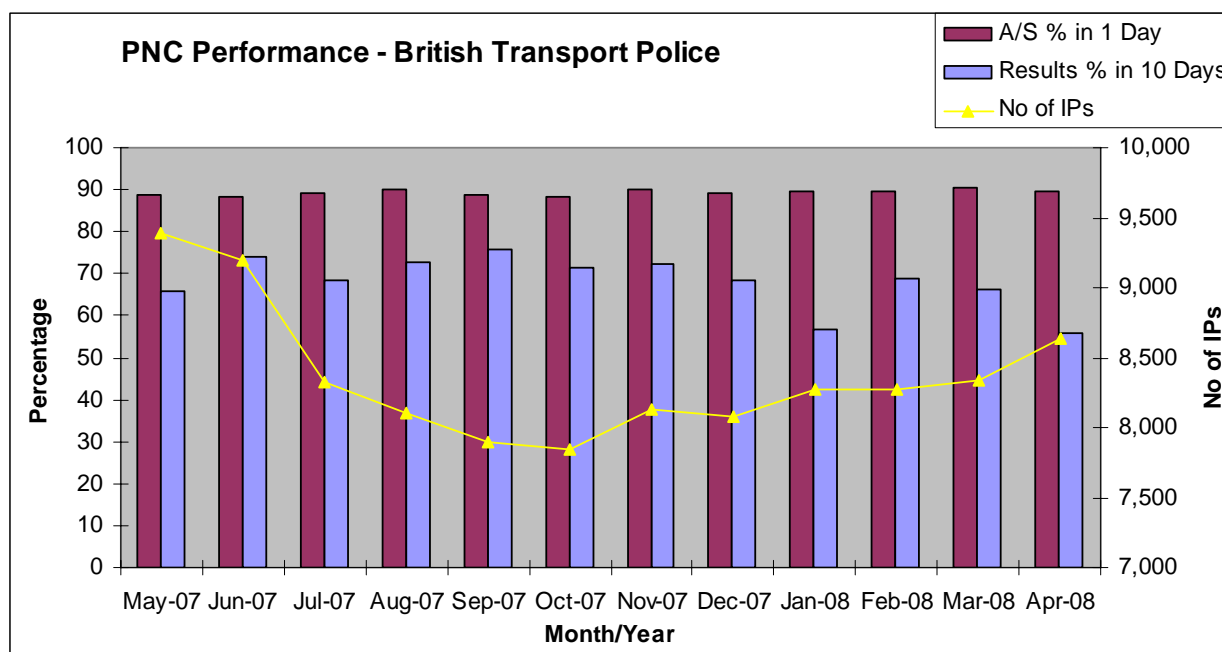
1.4.4 Whilst the legislation surrounding the PNC Code of Practice does not apply to British Transport Police, they are keen to embrace it, as the principles of the code are a good foundation to enable effective management of data that is processed on the PNC

1.4.5 In the 12 months to April 2008 the BTP performance against the ACPO target of entering 90% of A/S reports in 24 hours was on or within 2% of the target. The days to enter the quickest 90% have been at 1 day since July 2007 indicating that the force has robust procedures surrounding this process.

1.4.6 The court resulting performance has been more inconsistent. There are a number of mitigating factors that will have affected the force performance. The historical problems surrounding the provision of disposals from the courts in England and Wales; the procedure in Scotland whereby the force is reliant on the Scottish court service entering the results onto their IT system which subsequently transfers the data to PNC and the roll out of the Libra system across the court service in England and Wales that has slowed down the provision of court registers to the Home Office police forces. It should be noted that despite these circumstances when considering the days to enter the quickest 75% of disposals the BTP performance for the last 12 months is above the combined average of England, Scotland and Wales.

1.4.7 Impending Prosecutions (IPs) on the PNC have shown an overall reduction in the 12 months to April 2008. of 9%. However, as can be seen from the chart below, the more recent trend is for the IPs to increase.

1.4.8 A graph illustrating the British Transport Police performance in each of these areas in the 12 months to April 2008 is shown below:



1.5 Conclusions

1.5.1 HMIC’s assessment of PNC compliance within the Force has been assessed as:

Excellent – Comprehensive activity of effective activity against all the protocol areas.

1.5.2 While the assessment is based on the detailed findings of the report, HMIC Auditors did not determine any areas of concern and were therefore able to focus the inspection activity on identifying aspects where the force would be able to adjust in order to maximise their use of the PNC application.

A summary of the good practice identified and the recommendations for improvement can be seen in Appendix A of this report.

2. Detailed Findings and Recommendations

2.1 Leadership

- 2.1.1 The ACC [Crime] is an active participant in the force PNC Steering Group [PSG] chairing the meetings. Previous reports by Her Majesty's Inspector of Constabulary including the thematic report "On the Record" have highlighted the crucial role of chief officer involvement in the PSG. This is one of the few areas of consistency in forces that are seen as performing well and its importance cannot be over emphasised. Whilst recognising the competing demands placed on chief officers and the constraints on their time, their role in driving PNC and data quality standards is vital to the force's overall performance in this area.
- 2.1.2 The PSG meets approximately bi-monthly and produces both comprehensive minutes and a regularly updated action plan. The PSG instigates sub-groups to deal with specific issues as and when the need arises. HMIC Auditors reviewed the minutes of previous meetings and are satisfied that the membership of the group and the content of the meetings were sufficient to ensure strategic management of the system and processes within the force.
- 2.1.3 In light of the improved PNC performance and the embedded processes and procedures that BTP employ, it is the view of the HMIC Auditors that the force may wish to review the frequency of the PSG meetings. In previous inspections HMIC Auditors have been comfortable with quarterly PSG meetings.
- 2.1.4 HMIC Auditors reviewed the level of accountability placed upon officers concerning the submission of data for update to the PNC and the use of management information to support this process. The force has a PNC "champion" in each of the BCU's who deal with both performance and PNC issues. Officers are actively chased via the POINTS system to ensure completion of the reports within 24 hours. If the report is not completed within 36 hours it becomes "overdue" and is then visible to all users of the POINTS system. Supervisors can see every crime and offender their staff are dealing with along with potential detections. They can also view individual officers' queues. At month end copies of the overdue lists, and statistics relating to reports that have had to be returned for poor data quality are escalated by the CRC supervisors to the PNC Bureau Manager for action and dissemination to the area performance champions.
- 2.1.5 Key staff, including those in the CRC have data quality performance targets integrated in to their Personal Development Record [PDR] of appraisal.

2.2 Policy and Strategy

2.2.1 With regard to policy and strategy, the inspection focused on three areas; PNC Policy & Strategy, Security, and Data Protection. Each of these themes is discussed in further detail below.

2.2.2 PNC Policy and Strategy

2.2.2.1 British Transport Police's PSG action plan is based on the 2 timeliness and 19 organisational standards contained in the PNC Code of Practice. The PSG action plan is a good basis for a strategic document but would benefit from an enhancement to include issues relating to the roll out of PDA's, the implementation of Libra and Bichard 7 Portal, the INI-Impact programme, the Police National Database [PND], other integrated systems such as the Violent and Sex Offenders Register [ViSOR] along with any recommendations arising from in force Data Protection reports and HMIC inspections. This will ensure it is a "living" document that changes to meet the needs of the organisation and enable the PSG to retain a strategic overview.

Recommendation 1

Her Majesty's Inspector of Constabulary recommends that the force develops the PNC Steering Group action plan to include issues from other IT systems that impact on PNC and recommendations from data protection reports and HMIC inspections.

2.2.2.2 HMIC Auditors were given copies of the force PNC policies including those relating to the use of PNC by users and a comprehensive policy dealing with misuse of police IT systems. Policies are available on the force intranet and every user signs a PNC policy document acknowledging their responsibilities after attending and completing PNC training courses.

2.2.2.3 BTP have ascribed to the nationally accredited security documentation that is currently being ratified by the National Police Improvement Agency [NPIA], and will implement the national documentation when it becomes available.

2.2.2.4 All BTP police stations are in the process of being security audited and risk assessed to give the force a baseline, ensuring physical security of sites and data centres. It is the intention to give each site manager advice and guidance as necessary and then carry out a formal inspection 3 months later. Divisional Commanders are apprised of progress and outcomes.

2.2.3 PNC Security

- 2.2.3.1 User access is a generic term used by HMIC Auditors to denote the creation, amendment and deletion of users from the PNC depending on the circumstances. New users would be created on the system when they complete training, changes made to the levels of access should be made if users change roles. Finally, users should be deleted if they leave the force, have no further need to access the system, or their skills are no longer current.
- 2.2.3.2 HMIC Auditors were informed that the ability to create, amend or delete users from the system is limited to the PNC Bureau Manager and one other member of staff who provides holiday cover. The force currently has approximately 1000 active users of PNC. Force policy states that the Human Resources Dept [HR] should pass details of staff that join, leave or move within the organisation to the PNC Bureau Manager on a monthly basis. The PNC Bureau Manager also checks the General Orders [GO's] for information relating to staff to ensure the PNC User data is up to date.
- 2.2.3.3 With regards to the creation of new users and defining the appropriate level of access, the force PNC trainers provide an e-mail to the PNC Bureau Manager, who on receipt makes the necessary changes to the PNC user groups. HMIC Auditors are satisfied that this process meets the standard.
- 2.2.3.4 The PNC has built in security measures where it can identify users who have not used the system for 180 days or more and automatically removes the access to the system. HMIC Auditors were informed that non-users are checked after 100 days within British Transport Police. Staff that lose their access are assessed by the PNC training staff before access to PNC is re-instated. HMIC Auditors consider it good practice to use this opportunity to reassess the user prior to reinstating their access. There have been substantial changes to the PNC so it is essential the PNC users' knowledge and skills are current and up to date.
- 2.2.3.5 In addition, HMIC Auditors were encouraged to find that the force carries out an annual independent 100% PNC user access audit covering staff changes and access levels. This negates the risk of any individual being able to make changes to system access with no independent auditing of the activity being carried out. Very few errors have been found in the audits due to the robust and embedded processes, in view of this the force may wish to re-examine the audit regime and reduce the sample size.
- 2.2.3.6 Transaction monitoring is a requirement of the ACPO Data Protection Audit Manual. It is a process where police officers and staff are asked to verify their reasons for performing transactions on the PNC and, as such, is an important activity in the prevention and detection of misuse or abuse of the system. At the time of the inspection British Transport Police were using an electronic facility known as PNC Guard. The software randomly generates transaction checks which are e-mailed to the PNC user concerned, who has to justify the reason for the check to their line managers who then sign off the paperwork and return it to the PNC Bureau Manager. Line managers are expected to review the source documents. Any fail to replies or

inadequate justifications are escalated to the Information Security Officer [ISO] and Professional Standards Department [PSD].

2.2.3.7 PSD has robust procedures to pro-actively manager computer misuse along with a comprehensive policy document, which is currently a draft but is due to be ratified and implemented in the near future.

2.2.3.8 The force currently has 450 PDA's issued and intend to roll this out to a significant number off officers in the near future. Most PDA's are configured to give access to PNC. As PNC Guard does not cover PDA's the same way as a desk top check, an email is generated to indicate that a PDA user is subject to transaction monitoring the force has bespoke software that allows them to see what users have accessed via their PDA's. It has a full audit trail and also records the justifications for PNC checks made via the PDA. HMIC Auditors encourage the force to make full use of this facility to ensure that the same level of transaction monitoring is carried out across the PDAs.

2.2.4 Data Protection

2.2.4.1 Data Protection Audits are carried out by the force PNC Auditor. Annually the PNC Auditor, the PNC Bureau Manager and the ISO risk assess the force's PNC usage and complete a risk assessment. Additionally they agree which audits are required and set an audit time table for the year. Once competed the audits are sent to the ACC [Crime] and the PSG, any relevant issues and recommendations are added to the PSG agenda.

2.2.4.2 The PNC Auditor enters all audit reports and recommendations on to a spreadsheet with follow up reminders. HMIC Auditors noted that the recommendations in the reports would benefit by adhering to the SMART [Specific, Measurable, Achievable, Relevant and Time bound] principles. It would enable the recommendations to be easily monitored and the force would be able to improve processes to reduce errors in the future.

2.2.4.3 Additionally the PNC Auditor completes an action plan for each audit which is sent to the Chief Inspector responsible for the relevant department. Non-compliance with action plans is escalated to Area Commanders and the PSG. To increase ownership by relevant departments the force may wish to review the audit action plans and change the onus for completing the action plan and the time scales to the Chief Inspector responsible for the department, with the PNC Auditor retaining the follow up and escalation part of the process.

2.2.4.4 The PNC Auditor carries out weekly checks on the quality of PNC data by dip sampling 100 records. The results of the dip samples then generate reminders when necessary about the importance of data quality. Where training issues are identified the PNC Auditor liaises with the PNC training department. The PNC Auditor has also carried out data quality workshops with staff in key areas such as the CRC.

2.3 People

2.3.1 PNC Awareness

2.3.1.1 During meetings and focus groups, HMIC Auditors found awareness of PNC, ViSOR, QUEST and VODS was generally good at all levels within the organisation. The force has recently re-instigated general refresher training courses for all police officers every 5 years and HMIC Auditors suggest that the force should consider including PNC awareness into this course.

2.3.1.2 HMIC Auditors are of the opinion the force would benefit from a marketing strategy which could be included in the PSG strategic action plan to ensure awareness levels remain high. The marketing of the PNC needs to be viewed as an ongoing process where a variety of strategies are employed to encourage interest and awareness in the PNC on a rolling programme basis.

Recommendation 2

Her Majesty's Inspector of Constabulary recommends that the force adopts a structured approach to marketing by way of a formal strategy to promote the effective use of the PNC.

2.3.2 Training

2.3.2.1 The force delivers the standard NPIA recommended PNC courses which are modular and have been adapted to suit British Transport Police needs. The courses are only delivered by PNC accredited trainers and are all classroom based. However due to the pressure to reduce abstraction levels of officers from front line duties the force are currently researching other methods of delivering PNC training. The force also "buys in" training from other forces as and when required.

2.3.2.2 PNC Courses are planned in advance. The IT Training Manager produces a training directory of courses every October which is sent to the area training units. A member of staff requiring PNC training submits an application form, authorised by their line manager to the area training unit requesting the required PNC course. The area training unit decide who attends the courses. Each area has a skills matrix to refer to enabling the decision making process. Successful requests for training are prioritised and entered onto a list and returned to the IT Training Manager via the Cedar Training Application System [TAS]². BTP have addresses the issue of non-attendees and cancellations to courses by making them a Key Performance Indicator [KPI]. These are followed up by the HR department.

2.3.2.3 The force provides refresher training on an ad-hoc basis. Each request for refresher training or re-assessment for PNC access is dealt with individually by assessment with an accredited PNC trainer who then decides the best delivery method for the training for that particular student.

² The Cedar Training application is a computer system which enables the force to record requests for training, list courses and delegates and holds individual training records.

- 2.3.2.4 The force uses the Kirkpatrick method of training evaluation. Approximately 6 weeks after the course is completed a questionnaire is sent to the student's line manager to ascertain whether or not the skills and knowledge learned on the course has been sufficient for the student and has transferred into the work place. The questionnaire's are sent out by email and are returned to the IT Training Manager for review before being passed to the Learning & Development Evaluation Team to be analysed.

2.4 Partnerships and Resources

- 2.4.1 British Transport Police have a unique UK wide remit and has excellent working relationships with Home Office police forces and courts as a result of the extraordinary efforts they make to maintain these communications and partnership links. Other forces however are often unaware of the specific processes and requirements that BTP need in order to function efficiently. This leads to British Transport Police regularly having to deal with duplicated Arrest Summons entries on PNC. The force is proactive in approaching this issue and in trying to educate other force custody staff as to their operational needs. HMIC Auditors encourage the force to emphasize this issue when training new officers so that they are confident of the correct procedures when working with custody staff in other forces.
- 2.4.2 The force faces a similar issue when dealing with the courts, consequently, a large amount of time is taken up trying to locate warrants and details of court results. This is caused by the courts automatically sending the warrants and results to the geographic force and not directing them to BTP. The situation surrounding court results should improve with the implementation automatic updating of court results through the Libra court system and the Bichard 7 Portal which is due to go live nationally from March 2009. The force enters bail conditions when they are made aware of them and can obtain the details from the courts.
- 2.4.3 Due to British Transport Police's national remit there is regular contact and liaison with every other police force and court within the UK, additionally they have a major role within counter-terrorism and dealing with travelling criminals. In view of this it is key they are a full partner in the IMPACT Programme that includes the new Police National Database [PND]. The exchange of intelligence between UK forces and the BTP is vital to support operational policing within the UK.
- 2.4.4 HMIC Auditors were made aware of anecdotal evidence of issues of officers occasionally having difficulty obtaining PNC checks carried out by control room staff when the PNC Bureau was closed. This is particularly relevant when officers need to obtain previous conviction checks prior to the issue of a police penalty notice. Control Room supervisors also act as the ViSOR duty officer out of hours at times when the Control Room is often at its busiest. As part of the force's review of how it handles calls for service it may be useful to reconsider its provision of specialist out of hours PNC and ViSOR capability, and move to extending the hours the PNC Bureau operates or incorporate additional functionality within call handling. Many Home Office forces have successfully incorporated this demand within a real time intelligence unit attached to the control room.

- 2.4.5 Both the PNC Bureau Manager and PNC Auditor attend national PNC meetings and Impact Data Quality meetings amongst others to ensure the force is kept up to date with national strategic PNC issues.
- 2.4.6 Throughout the week of the inspection, it was clear that the PNC Bureau Manager and who is also the PNC Liaison Officer, is held in high regard throughout the force in terms of the work and knowledge of the PNC. Although this is seen as a strength in the short term, it was felt that this could be a potential weakness for the Force as there was no similar role anywhere in the Force. The PNC Liaison Officer carries out a number of administrative functions, prepares the key performance figures, offers advice and guidance concerning PNC, all of which would need to continue if the current post holder was no longer available.

Recommendation 3

Her Majesty's Inspector of Constabulary recommends that the force explores options to ensure that the essential functions carried out by the PNC Liaison Officer can be maintained in the organisation as part of the Business Continuity Plan.

2.5 Processes

- 2.5.1 On 1st January 2005 the performance indicators of the ACPO Compliance Strategy were replaced by the timeliness standards contained in the newly published Code of Practice for the PNC. The PNC Code of Practice developed by the National Centre for Policing Excellence and endorsed by ACPO, is a statutory code made under s.39a of the Police Act (inserted by section 2 of the Police Reform Act 2002). The legislation is made under law covering England and Wales and the Code stipulates that 90% of recordable offences be entered onto the PNC within 24 hours of the commencement of proceedings. The commencement of proceedings is defined as when a person is arrested, reported or summonsed.
- 2.5.2 While the law governing the Code of Practice does not specifically apply to the British Transport Police, the principles of the Code are a good foundation for the effective management of data being processed on the PNC. HMIC Auditors are pleased to note that British Transport Police use the Code as their target for arrest summons (A/S) report entry.
- 2.5.3 Feedback from interviews and focus groups indicated that officers were aware of the 24 hour submission requirement for Source Input Documents [SID's] which are electronic [E-SID's] within British Transport Police and are robustly and effectively managed via the POINTS system. Overdue E-SID's, poor quality E-SID's or non-submission of E-SID's are reported back to area, followed up and included as a performance measure within the force.
- 2.5.4 HMIC Auditors conducted reality checks of records updated by British Transport Police operators in order to verify the quality of data being entered on to the PNC. The quality of information is important for the success of QUEST searches on the PNC. Of the records that were checked against E-SIDS none were found to contain significant errors.

- 2.5.5 British Transport Police's data was further checked to see if it held any records where the offender was under the age of 5 or described as "sex unknown". Again no errors were found that were attributable to British Transport Police.
- 2.5.6 Nineteen court results were checked against PNC. One error relating to a missed court order was noted and highlighted to the force for correction.
- 2.5.7 CRC staff were extremely keen to give the best service possible to officers and members of the public and highlighted that they weren't always sure that they had searched the PNC Property file efficiently. Subsequent discussions revealed that they were unaware of the Property Online Descriptive Search [PODS] functionality of PNC as it wasn't included in their training. The force should review the training given to CRC staff to include the PODS functionality in future and arrange for existing staff to be trained.

Recommendation 4

Her Majesty's Inspector of Constabulary recommends that the force reviews and develops its PNC Property course module for CRC staff to include the Property Online Descriptive searching functionality and arranges appropriate training for new and existing staff.

- 2.5.8 HMIC Auditors also considered the quality of information being entered on the originator line of PNC. The originator line is a free text field to record the reason why a transaction is taking place. It can be used as a tool for supervisors who are managing PNC users to ensure that all transactions are for a legitimate policing purpose. The information on the originator line can also be used during investigations, when a history of transactions is being researched. HMIC Auditors are satisfied that there is adherence to the force policy.
- 2.5.9 The force does not currently use PNC Crimelink. However ongoing issues with cable theft around the UK and a recent serious cross border investigation have highlighted the usefulness of placing apparently unrelated and unsolved cases on to Crimelink to facilitate searching for similarities and links. HMIC Auditors therefore encourage the force to review its use of the Crimelink application.
- 2.5.10 Ad hoc intelligence updates is information applicable for update to PNC that originates from a source other than the creation of an arrest summons report. This is an area where the force could make a difference. HMIC Auditors are not reassured that the current processes capture all relevant and useful intelligence on to PNC. While ad-hoc intelligence from officers and large incidents are entered on the force intelligence system or on the HOLMES system but not are captured on PNC which is the only truly national system.

Recommendation 5

Her Majesty's Inspector of Constabulary recommends that the force establish a process to record ad hoc intelligence information onto the PNC.

2.6 Results

- 2.6.1 Though not bound by the targets incorporated in the Codes of Practice British Transport Police have consistently entered between 88.1% and 91.7% of their arrest summons reports onto PNC within 24 hours from May 2007 to April 2008.
- 2.6.2 Performance with regard to the input of court results has shown a generally downward trend over the last 6 months declining from 75.8% in September 2007 to 56.1% in May 2008. In the previous 6 months the force had seen a continuous trend of improvement in court results increasing from 65.8% in May 2007 to 75.8% in September 2007. The downward trend in the inputting of court results may be in part attributable to the implementation of the Libra system into magistrates' courts in England and Wales. As each court area has migrated to Libra since October 2007 the local geographic forces have in general experienced delays in receiving court results. As the only national Force British Transport Police is suffering from the cumulative effect of these delays.
- 2.6.3 The number of Impending Prosecutions outstanding is 8837 in April 2008 which is high when compared to forces of a similar size to British Transport Police, this could be attributed to the effects of Libra and the Scottish court procedure but further work is required by the force to fully establish the reasons. HMIC Auditors were made aware that the force has set up an Impending Prosecutions Sub Group to investigate the issue and to put in place policy and procedures to write off offences where the result is unobtainable.
- 2.6.4 The recommendations outlined in this report aim to improve the quality of the data being input and to assist British Transport Police in obtaining maximum benefit from the PNC.

Appendix A

Summary of Recommendations for British Transport Police

Recommendation 1

Her Majesty's Inspector of Constabulary recommends that the force develops the PNC Steering Group action plan to include issues from other IT systems that impact on PNC and recommendations from data protection reports and HMIC inspections.

Recommendation 2

Her Majesty's Inspector of Constabulary recommends that the force adopts a structured approach to marketing by way of a formal strategy to promote the effective use of the PNC.

Recommendation 3

Her Majesty's Inspector of Constabulary recommends that the force explores options to ensure that the essential functions carried out by the PNC Liaison Officer can be maintained in the organisation as part of the Business Continuity Plan.

Recommendation 4

Her Majesty's Inspector of Constabulary recommends that the force reviews and develops its PNC Property course module for CRC staff to include the Property Online Descriptive searching functionality and arranges appropriate training for new and existing staff.

Recommendation 5

Her Majesty's Inspector of Constabulary recommends that the force establish a process to record ad hoc intelligence information onto the PNC

Appendix B

Summary of Good Practice at British Transport Police

- The ACC [Crime] is an active participant in the force PNC Steering Group [PSG] chairing the meetings. This is considered good practice as the role of chief officers driving improvements to data quality is seen as crucial.
- The PSG instigates sub-groups to deal with specific issues as and when the need arises. This is recognised as good practice.
- Officers are actively chased via the POINTS system to ensure completion of the reports within 24 hours. If the report is not completed within 36 hours it becomes “overdue” and is then visible to all users of the POINTS system. They can also view individual officers’ queues. At month end copies of the overdue lists, and statistics relating to reports that have had to be returned for poor data quality are escalated by the CRC supervisors to the PNC Bureau Manager for action and dissemination to the area performance champions. The use of the POINTS system to manage the submission and data quality of e-SID’s is recognised as good practice.
- Key staff, including those in the CRC have data quality performance targets integrated in to their Personal Development Record [PDR] of appraisal.
- The force carries out an annual independent 100% PNC user access audit covering staff changes and access levels. This negates the risk of any individual being able to make changes to system access with no independent auditing of the activity being carried out.
- The PNC has built in security measures where it can identify users who have not used the system for 180 days or more and automatically removes the access to the system. HMIC Auditors were informed that non-users are checked after 100 days within British Transport Police. Staff that lose their access are assessed by the PNC training staff before access to PNC is re-instated. HMIC Auditors consider it good practice to use this opportunity to reassess the user prior to reinstating their access. There have been substantial changes to the PNC so it is essential the PNC users’ knowledge and skills are current and up to date
- As PNC Guard does not cover PDA’s the force has bespoke software that allows them to see what users have accessed via their PDA’s. It has a full audit trail and also records the justifications for PNC checks made via the PDA’s.
- The PNC Auditor has also carried out data quality workshops with staff in key areas such as the CRC to highlight and improve data quality.

Appendix C

Thematic Inspection Report on Police Crime Recording, the Police National Computer and Phoenix Intelligence System Data Quality - 'On The Record'

Recommendation 9 (Chapter 5 page 86)

Her Majesty's Inspector recommends that all Forces produce position statements in relation to the 1998 PRG report recommendations on Phoenix Data Quality and the ACPO Compliance Strategy for the Police National Computer. He further recommends that Forces produce a detailed action plan, with timescales, to implement their recommendations. The position statements and action plans together with progress updates should be available for audit and inspection during future HMIC PNC Compliance Audits and inspection of Forces. Forces should send copies of action plans to HMIC's PNC Compliance Audit Section by 1 February 2001.

Recommendation 10 (Chapter 6 page 104)

Her Majesty's Inspector recommends that Forces urgently review their existing SCAS referral mechanisms in the light of the above findings. These reviews should include verification with SCAS that all Force offences fitting the SCAS criteria have been fully notified to them, and updated. This process should be managed by Forces through their in-Force SCAS Liaison Officers.

Recommendation 11 (Chapter 7 page 111)

Her Majesty's Inspector recommends that the marketing, use and development of national police information systems is integrated into appropriate Force, local and departmental, strategic planning documents.

Recommendation 12 (Chapter 7 page 112)

Her Majesty's Inspector recommends that where not already in place, Forces should establish a strategic PNC Steering Group. This group should develop and be responsible for a strategic plan covering the development, use and marketing of PNC and Phoenix.

Recommendation 13 (Chapter 7 page 118)

Her Majesty's Inspector recommends that all Forces conduct an audit of their present in-Force PNC trainers to ensure they have received nationally accredited training. Any individuals who have not been accredited as PNC trainers by National Police Training should not conduct in-Force PNC training.

Recommendation 14 (Chapter 8 page 145)

Her Majesty's Inspector recommends that Forces ensure that each Phoenix inputting department develops an audit trail to register the return of substandard PSDs, via line supervisors, to originating officers. The system developed should include a mechanism to

ensure the prompt return of PSDs. Forces should also incorporate locally based audit trails, monitoring the passage of returned PSDs between line supervisors and originating officers.

Recommendation 15 (Chapter 8 page 146)

Her Majesty's Inspector recommends that Forces develop clear guidelines to cover their expectations of officers on the return of incomplete or substandard PSDs. This guidance should be communicated to all staff and regular checks conducted to ensure compliance.

Recommendation 16 (Chapter 8 page 148)

Her Majesty's Inspector recommends that Forces should develop a system to ensure that all ad-hoc descriptive and intelligence updates registered on local Force systems are automatically entered onto the Phoenix system. The policy should clearly outline whose responsibility it is to notify Phoenix inputters of any descriptive changes. Forces should also ensure that the policy is marketed to staff and that regular checks are conducted to ensure compliance.

Recommendation 17 (Chapter 8 page 150)

Her Majesty's Inspector recommends that Forces develop a formal system to ensure that a proportion of each member of Phoenix inputting staff's work is regularly checked for accuracy. Forces should also consider the benefits of measuring other aspects of their work including speed of entry and compliance with policies. Performance outcomes should be evidenced in staff PDRs.

Recommendation 18 (Chapter 9 page 164)

Her Majesty's Inspector recommends, where not already present, that Forces develop risk assessed Force Data Protection Officer audit programmes.

Recommendation 19 (Chapter 9 page 164)

Her Majesty's Inspector recommends that Forces integrate PNC and Phoenix data quality compliance into their performance review and inspectorate programmes for BCUs and specialist departments.

Recommendation 20 (Chapter 9 page 165)

Her Majesty's Inspector recommends that PSD performance statistics should be incorporated in routine Force performance information. The statistics should identify omissions and errors in individual fields, in particular, descriptive information. Appropriate accountability measures should be established to ensure that any performance shortfalls identified are addressed.

Appendix D

PRG Report “Phoenix Data Quality” Recommendations

- National performance indicators and standards for timeliness of input, data fields to be completed, quality assurance requirements and the provision of training should be agreed by ACPO and promulgated to all Forces.
- Achievement against and compliance with these indicators should be audited after a period of 12 months, perhaps through the inclusion in the scope of HMIC audits.
- Senior officers take an active and visible role in policing compliance with agreed standards within their own Force.
 - ACPO performance indicators should be reflected in Force policy or standing orders (or the Force equivalent). Guidance should include the responsibilities of officers at each stage of the process e.g. for the provision of source documentation, for approval, time taken to pass to input bureaux, and the bureaux' responsibilities for data entry and quality control.
 - Line and divisional managers, as well as chief officers, should be held accountable for compliance with these standards. This could be achieved through inclusion in divisional efficiency assessments, and through the publication and dissemination of performance statistics throughout individual Forces and nationally.
- Source documentation should be common across all Forces, if not in design, in the information requested. A national format, stipulating a hierarchy of fields to be populated, should be developed.
- Programme(s) geared to raising awareness amongst operational officers and line managers of the potential benefits of Phoenix in a practical sense and their responsibilities of the provision of data should be developed. To ensure all officers have an opportunity to benefit from these programmes, consideration should be given to inclusion of a 'Phoenix awareness' module in probationer training, promotion courses and divisional training days.
- Best practice in administrative arrangements and organisational structures should be widely distributed. Internal working practices and organisational structures should be streamlined to remove any redundancies.

- Greater computerisation of the transfer of results from courts direct to Phoenix should continue to be developed. In the shorter term, the Police Service is likely to retain responsibility of the input of court information. To minimise the resource burden on the Police Service in this interim period, the police and courts should work to ensure recognition of each other's requirements and to minimise any inconsistencies in their respective working practices.
 - In the first instance, this might be achieved by ACPO highlighting to Magistrates' Courts and to the Crown Court, perhaps through the Trials Issue Group, the importance of Phoenix records to the integrity of the criminal justice system as a whole. Liaison meetings could usefully be established to introduce greater consistency in working and recording practices between the courts and police Forces e.g. for recording data. In the first instance, this could be pursued locally, perhaps through the court user group. Issues considered by such meetings might include supplying additional information (such as Arrest / Summons numbers) to the Magistrates' Court system and to automated transfer of court registers.
 - Consistent practice and performance is also required from the courts. Recommendations referring to performance indicators and standards, audits and monitoring, senior level commitment, common recording practices, awareness of system customers and administrative 'best practice' could equally apply to the courts. Mirroring the responsibilities of Chief Constables for their Force, the Court Service and the Magistrates' Court Committee should be accountable for the performance of courts.
 - Consistent practice in advising custody details, including transfers and releases, is required. This includes consistency in advising CRO numbers to maximise the number of complete records. The police and prison services should liaise to encourage greater understanding and acknowledgement of each other's requirements.

Appendix E

Police National Computer Data Quality and Timeliness – 1st Report

Recommendation One (Paragraph 5.2)

Her Majesty's Chief Inspector recommends that ACPO nationally review the position and priority of PNC within the structure of portfolio holders to reflect both the technical and operational importance of PNC.

Recommendation Two (Paragraph 5.11)

Her Majesty's Chief Inspector draws renewed attention to Recommendations 11 to 20 of '*On the Record*' (2000), and recommends that all forces develop appropriate systems, overseen at a senior level, to ensure that they are implemented.

Recommendation Three (Paragraph 5.19)

Her Majesty's Chief Inspector recommends that PITO review, as a matter of urgency, the supplier/customer relationship between PNC and forces, particularly in relation to the marketing of PNC functionality, and the type, frequency and validity of management information reports produced.

Recommendation Four (Paragraph 5.29)

Her Majesty's Chief Inspector recommends that Her Majesty's Inspector (Training), in consultation with PITO and National Police Training, conducts a review of the quality and availability of accreditation training for PNC trainers and the extent to which they are subsequently employed in forces.

Recommendation Five (Paragraph 5.31)

Her Majesty's Chief Inspector recommends that discussions take place between ACPO, PITO and other relevant stakeholders to examine what opportunities exist for a short term 'technology solution' for the inputting of Court Results, either involving NSPIS applications currently in development, or an interim solution.

Recommendation Six (Paragraph 5.34)

Her Majesty's Chief Inspector recommends that renewed and re-invigorated discussions should take place between relevant stakeholders to, (a) Ensure that local systems are in place to maximise co-operation with the courts to achieve their respective 72 hours targets and, (b) Work towards Magistrates' Courts and Crown Courts assuming full responsibility for inputting all case results directly onto PNC.

Recommendation Seven (Paragraph 6.10)

Her Majesty's Chief Inspector recommends that following appropriate consultation with relevant stakeholders, a national inspection protocol for PNC data quality and timeliness be introduced.

Recommendation Eight (Paragraph 6.12)

Her Majesty's Chief Inspector recommends that following appropriate consultation with relevant stakeholders, the Secretary of State should consider using his powers under Section 5 of the Local Government Act 1999, to require all police authorities to institute a Best Value Review of processes to ensure PNC data quality and timeliness. Such review should be conducted against a common template and terms of reference.

Recommendation Nine (Paragraph 6.14)

Her Majesty's Chief Inspector recommends that in consultation with the Standards Unit and other stakeholders, HM Inspectorate should urgently review their current PNC audit responsibilities in the light of the findings of this report, with a view to adopting a more proactive stance in relation to force performance, data quality and timeliness.

Recommendation Ten (Paragraph 6.16)

Her Majesty's Chief Inspector recommends that in consultation with other stakeholders, ACPO IM Committee initiate research with a view to encouraging mutual support between forces for out of hours PNC data entry purposes.

Appendix F

Police National Computer Data Quality and Timeliness – 2nd Report

Recommendation 1

The Home Office should lead and co-ordinate an urgent re-examination of the current PNC strategy and standards with a view to producing national binding performance and compliance criteria to which all relevant stakeholders and partners are agreed and committed.

Recommendation 2

ACPO nationally and Chief Constables locally must ensure that the national standards for PNC operation, resourcing and training are fully integrated into local Information Management Strategies and recognised as an important part of operational service delivery. This area must receive sustained high-level support through a 'champion' at chief officer level.

Recommendation 3

PITO should be tasked to consolidate the force 'profiling' approach as used in the inspection into the routine statistical returns provided to forces. PNC statistics should then be integrated into the mainstream suite of management information/indicators that inform decisions at force and BCU levels.

Recommendation 4

HMIC should be tasked to establish a risk-assessed programme of monitoring and inspection that is able to respond quickly and effectively to deviations from accepted standards. This programme should include;

- remote monitoring of performance (PITO profile statistics)
- regular collaboration and contact with force PNC Managers
- proportionate programme of visits and inspections
- targeted interventions to respond to identified problems

Recommendation 5

The Home Office should establish a structured process for addressing and remedying any significant and persisting deviation from the agreed national standards (see Recommendation 1). This process should identify the respective roles of HMIC, Police Standards Unit and police authorities. It should set out the escalation of responses, which might include an agreed action plan, re-inspection, Intervention, and ultimately withdrawal of facility.