WEST MIDLANDS POLICE

21 – 28 NOVEMBER 2005

POLICE NATIONAL COMPUTER COMPLIANCE REPORT

Table of Contents

1. Executive Summary

1.1 Introduction

1.1.1 Her Majesty's Inspectorate of Constabulary (HMIC) conducted a Police National Computer (PNC) Compliance Inspection of West Midlands Police (WMP) between 21st and 28th November 2005.

1.1.2 The Constabulary was subject to a PNC Compliance Audit using the revised July 2005 Protocols on PNC Compliance. Her Majesty's Inspector would like to acknowledge the enthusiasm of the Force and also to place on record his thanks to all members of staff who contributed to this report and provided assistance during the inspection.

1.1.3 This report is based on views and comments obtained from strategic, PNC and customer level management and users at Force Headquarters and at 6 of the 21 Basic Command Units (referred to as Operational Command Units - OCUs). These views have been supported by reality checks conducted by HMIC PNC Compliance Auditors (hereafter referred to as HMIC Auditors).

1.2 Background

1.2.1 West Midlands Police is the second largest police force in the country in terms of police officer establishment, behind London's Metropolitan Police Service. The WMP cover an area of 384 square miles and serves a population of almost 2.6m people. The region sits at the very heart of the country and covers the three major cities of Birmingham, Coventry and Wolverhampton. The regions economy is presently diverse and much of its heavy industries date back to the Industrial Revolution. The region is well served by rail and road links. An average of 170,000 people travel through it daily on the M5, M6 and M42 motorways making it one of the busiest motorway networks in Europe. The population of the West Midlands is very diverse with approximately 10% being born outside the UK. The average earnings and house prices for the region are lower than the national averages.

1.2.2 Force headquarters is located at Lloyd House, in the heart of Birmingham city centre. The Force is headed by the Chief Officer Group comprising the Chief Constable, the Deputy Chief Constable, four Assistant Chief Constables with portfolios covering crime, criminal justice and IT, operations and intelligence, and Directors of finance and personnel. In terms of staff numbers WMP employs around 8,150 police officers, 3,150 police staff, 110 police community support officers and 950 special constables.

1.2.3 The PNC Bureau (PNCB) located within the police headquarters operates a 24/7 PNC service to the whole Force for transaction enquiries, the VODS (Vehicle on Line Search) and QUEST (Queries Using Extended Search Techniques) searches. This provided additional cover for the OCUs who have VODS and QUEST capabilities during extended office hours. The PNCB also creates the wanted missing reports (except warrants and anti-social behaviour orders), disqualified driver reports and confirms and removes vehicle and property reports.

The DVLA liaison is a separate role but operates largely under the umbrella of the PNCB. It has a close liaison with data protection and Performance Review as well as IT training in the identification of best practice within the module content. The Bureau manages the PNC user access which includes resetting passwords and unlocking terminal. It maintains the PNC website and is generally regarded as a centre of excellence for advice on PNC related topics.

1.2.4 WMP are using a custody system called ICIS which interfaces with the PNC to create the arrest summons (A/S) report. The custody sergeant creates the custody record on ICIS when the offenders enters the custody unit. It is then updated by the arresting officer with the full charge and description details. Once the offender has been formally charged and given a disposal from ICIS the custody officer has the facility to send the information to the PNC to create the A/S record. The system is set up with both time prompts and a prompt once the record is disposed from ICIS to reminder the ICIS operator to send the record to the PNC.

1.2.5 The responsibility for ensuring all the records transfer to the PNC lies with the OCU staff. Historically this 'message maintenance' role was the responsibility of the Data Handlers in the OCUs. The need to make this a 24/7 function was identified to enable the WMP to attain the A/S target of 90% within 24 hours and as a result, custody officer assistants (COAs) were trained in some OCUs to carry out this function over the weekends. This is not a 24/7 function in 2 out of the 6 OCUs that were visited.

1.2.6 Court results are updated onto the PNC in 14 locations throughout the WMP. Eleven of these are Glidewell locations, where WMP staff work alongside staff from the crown prosecution service (CPS). The majority of court registers are received via secure email, a small minority of court resulting units rely on paper copies of the court register being received

1.2.7 The Crown Court results are received via the Xhibit application, but unfortunately the system does not supply complete details of indictments so the Force has to wait until hard copies of these are received in order to update the PNC record.

1.3 Methodology

1.3.1 A full inspection against the 2003 PNC Protocols was carried out, covering the sections of Leadership, Policy and Strategy, People, Partnerships and Resources, Processes and Results.

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

- **Excellent** – Comprehensive evidence of effective activity against all protocol areas.

- **Good** – Evidence of effective activity in 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 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 its adherence to the protocols. This was followed up by a visit to the Force with HMIC Auditors conducting numerous 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 reviewing PNC data against source documents and a review of PNC policy documentation.

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.

1.4 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 Centrex, HMIC, Police Information Technology Organisation (PITO) and individual 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.

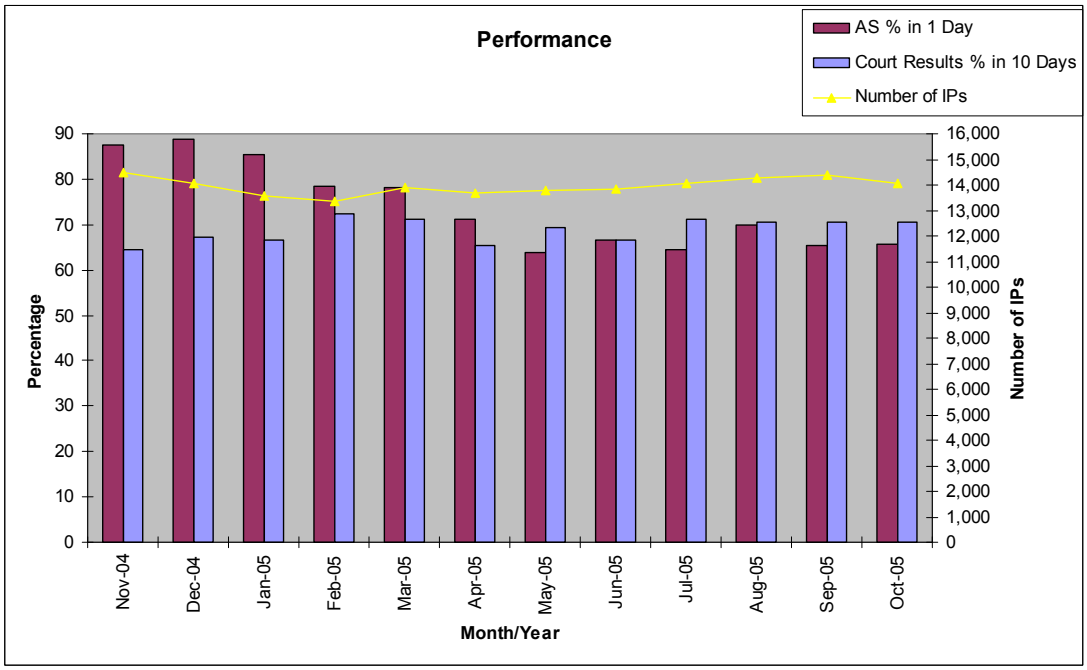
- From the 1st July 2005, the target is for 75% of all finalisations being entered onto PNC within 7 days of the information being received by the police. For the previous 6 months the target was for 50% of the court results to be entered within 7 days. Courts have their own target of 3 days for delivery of data to the police. Therefore, the police are measured against an overall target of 10 days.

1.4.4 In October 2005, WMP input 65.7% of Arrest/ Summons (A/S) updates on the PNC within 24 hours. This shows a deterioration in performance in the previous 12 months as the Force input 87.4% in November 2004. It is understood that this disappointing performance is as a consequence of the Force adopting the full powers of the 2003 Criminal Justice Act which has resulted in an approximate 35% increase in the number of A/S reports that the Force has to process on a monthly basis. The Force are currently testing an electronic solution to the ICIS system which will enable them to transfer all custody records to the PNC at the point of arrest. HMIC Auditors are reassured that the Force was close to achieving the 90% prior to the adoption of the 2003 CJ Act. They therefore look forward to the Force returning to the previous A/S report input performance levels once they have implemented the ICIS application electronic solution.

1.4.5 The WMP's performance in terms of court results is of concern as the Force has not achieved the 75% target since it was introduced in July 2005. In the previous six months the Force comfortably achieved the 50% target but has not been able to improve sufficiently to reach the revised performance target.

1.4.6 In terms of Impending Prosecutions (IPs) WMP have shown a slight increase in the 12 months to October 2005 from 14,041 to 14,511. The percentage increase for this period is 0.03%.Whilst this is a satisfactory position which demonstrates the processes are enabling the Force to maintain the level of IPs they have outstanding, HMIC auditors are aware that WMP have a approximately 4,000 custody records waiting to be recorded onto the PNC as a result of the way in which the Force has decided to record CJ Arrestees onto the PNC. These IPs will be created on the PNC once the electronic solution mentioned in 1.4.4 is activated. Therefore, WMP will need processes in place to ensure that these IPs are resulted within an appropriate timescale.

1.4.7 A graph illustrating WMP's performance in the 12 months to October 2005 is shown below*:*



1.5 Conclusions

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

Fair – Evidence of effective activity covering some areas, but concerns in others.

1.5.2 This assessment is based on the detailed findings of the report which highlight concerns in several areas of activity:

- the arrest summons performance:
- currently WMP are unable to completely justify their performance against the ACPO PNC Code of Practice in relation to the input of court results:
- the Quality Improvement Process is in its infancy and has yet to embed into the Force culture, leaving WMP exposed to the risk of limited auditing.

1.5.3 The findings of this report should be read in conjunction with the previous reports and recommendations relating to the PNC. The previous reports are:

- Police Research Group Report – 'Phoenix Data Quality', *published 1998*
- HMIC Thematic Inspection Report – 'On The Record', *published 2000*
- HMIC Report – 'PNC Data Quality and Timeliness, 1st Report', *published 2001*

- HMIC Report – 'PNC Data Quality and Timeliness, 2nd Report', *published 2002*

1.5.4 A summary of good practice points, along with recommendations for improvement can be found at Appendices A and B of this report.

2. Detailed Findings and Recommendations

2.1 Leadership

2.1.1 Role of the PNC Strategy Group

2.1.1.1 The HMIC Auditors were encouraged to find leadership in relation to the PNC, to be an area of strength within the Force. Although there are two ACCs whose portfolios cover the PNC arena there was evidence of effective strategic management. In addition, there was evidence during interviews of good levels of knowledge and understanding with regard to PNC issues. HMIC Auditors were pleased to note that the PNC Liaison Officer had good access to the ACCs when strategic decisions were needed.

2.1.1.2 There is an established PNC Strategy Group which meets regularly with well laid out Terms of Reference. The meeting is always chaired by a Chief Officer.

2.1.1.3 All the operators and users of the PNC have their own regular subcommittee meetings. The OCU Data Managers, the Ops Centre Managers, the Community Safety Bureau (CSB) mangers and the ICIS User Group all meet regularly and independently of each other. They all manage staff who update and or make enquiries of the PNC.

2.1.1.4 In previous inspections HMIC Auditors have acknowledged good practice where there is a PNC User Group that interacts with the PNC Strategy Group. Whilst it is recognised that to suggest an additional meeting would add an additional burden into the already busy meeting schedule at WMP, making PNC a standing agenda item within the meeting structure would ensure that the major users of the PNC are kept up to date and have the ability to input into the PNC Strategy Group.

Recommendation 1

Her Majesty's Inspector of Constabulary recommends that the Force ensures that Data Managers meetings, the Ops Centre Managers meetings, the CSB managers meetings and the ICIS User Group include PNC as a standing agenda item, to ensure that there is an interaction between them and the PNC Strategy Group.

2.1.2 Responsibility and Accountability

2.1.2.1 With regard to the overall Force performance against the ACPO PNC Code of Practice, performance statistics are produced at the OCU level and form part of the bi-monthly Performance Improvement Conference which is chaired by the DCC. The performance data was made available to the HMIC Auditors as part of the pre-read material prior to the inspection. However, the headings on the charts were unclear as to the information being presented, it is suggested that the titles clearly

explain the data being displayed so that the impact is not lost on the reader.

2.2 Policy & Strategy

2.2.1 PNC Policy and Strategy

2.2.1.1 HMIC Auditors were provided with a copy of the Force's Strategic Action Plan for PNC. This document outlines the Force's aims with regard to PNC and states how these aims are to be achieved. This document is viewed within the Force as a working document and is therefore regularly updated. Having such a document in place is established good practice.

2.2.1.2 The HMIC Auditors were able to view the comprehensive set of PNC policy documents available on the Force intranet. This is also viewed as good practice.

2.2.1.3 Feedback from interviews and focus groups cause HMIC Auditors to tender a note of caution over reliance simply by publishing policy on the intranet where interpretation is down to the OCUs. The message maintenance function of the ICIS application is an example of where policy dictates that 24/7 cover should be available, yet the evidence is that this is not always the situation.

Recommendation 2

Her Majesty's Inspector of Constabulary recommends that the Force ensures that there is compliance in the OCUs to the PNC policy documents.

2.2.2 PNC Security

2.2.2.1 With regard to system security, HMIC Auditors reviewed five key areas. These are User Access, Transaction Monitoring, Data Protection Auditing, the Role of Professional Standards and the role of the Information Security Officer. Each of these is discussed further below and raised some areas of good practice but also some areas of concern.

2.2.2.2 User access to the PNC in WMP is managed by the DVLA Liaison who retains a list of all active users on the system. Access is granted following the successful completion and subsequent assessment at the end of a training course. A list of successful candidates is sent to the DVLA Liaison via email from an accredited trainer so the administrator can make the necessary updates to the user groups.

2.2.2.3 There is also a process to ensure that all officers and staff who leave the organisation or change job roles, thus no longer requiring access to the PNC, have their access to the PNC either deleted or changed. These processes are viewed as sufficiently robust to ensure that only legitimate users have access to the system.

2.2.2.4 Nevertheless, one area for improvement to the current system was identified during the inspection. Whilst HMIC Auditors do not question the integrity of the work of the DVLA Liaison there is some risk to the organisation where the department carrying out this function is operational and the process is not independently audited.

Recommendation 3

Her Majesty's Inspector of Constabulary recommends that WMP introduces an independent audit, at least annually, of all user access administration.

2.2.2.5 The undertaking of 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 PNC. Currently WMP are not undertaking this process. Instead they are monitoring the information supplied on the originator line which is completed each time a PNC check is requested. The information contained within the originator line can validate the PNC check and it can be used for intelligence purposes.

2.2.2.6 Whilst it is commendable that WMP are improving the quality of the data entered onto the originator line and once this improves validation audits will recommence, the transaction monitoring as required by the ACPO Data protection Audit Manual is not being undertaken by WMP.

Recommendation 4

Her Majesty's Inspector of Constabulary recommends that the Force recommences the process of PNC transaction monitoring in line with the ACPO Data Protection Audit Manual.

2.2.2.7 WMP is in the process of changing the PNC auditing function. It is in the early stages of implementing a procedure known as Quality Improvement Process (QIP). OCU staff are being trained to audit the data quality of the PNC updates made by their own staff. The results are fed into a standard report format which is then collected by the central Information Compliance Unit. The process was in its infancy at the time of the inspection so not all the OCUs had been trained and the audit process only covered the Wanted/Missing reports updated by the OCU operators.

2.2.2.8 HMIC Auditors consider this to be an innovative initiative to PNC auditing. However, as it is still in its early stages the Force is exposed to the risk involved in limited auditing, both in the amount being carried out and in the PNC areas that are covered. The Force needs to assure itself that there is sufficient audit coverage across the PNC applications throughout all the OCUs to ensure data quality and integrity is maintained.

Recommendation 5

Her Majesty's Inspector of Constabulary recommends that the Force ensures that it undertakes sufficient auditing to comply with the PNC Code of Connectivity whilst it is embedding the Quality Improvement Process.

2.2.2.9 HMIC Auditors were informed that the Information Security Policy is reviewed annually which is seen as good practice.

2.2.2.10 There are online computer based training packages available via the intranet covering both Data Protection and Information Security. However, HMIC Auditors were informed that the Data Protection Officer (DPO) has no input to the IT training department which delivers data protection as part of the PNC courses. The DPO will have access to the most up to date information in this area and would be in the best position to ensure that the IT trainer's material is accurate.

2.2.2.11 WMP also have a policy of regularly reviewing the use staff make of their PNC access. If the PNC enquirer has not accessed PNC for 6 months they will be removed from the system and will either have to retrain or resit the PNC assessment before their access is reinstated.

2.2.2.12 HMIC Auditors also reviewed the role of the Professional Standards Department (PSD) with regard to PNC issues at WMP. The PSD is independent of operational activities. Such independence is viewed as good practice. Within the PSD there is a unit which has 2 PNC trained

operators to enable them to conduct investigations involving PNC activity, but they sometimes need to involve the PNCB supervisor in the more complex investigations, which has the potential to risk the independence of the investigations involving the PNC.

2.3 People

2.3.1 Marketing and Awareness

2.3.1.1 During meetings and focus groups, HMIC Auditors were concerned about the variable levels of awareness of some of the functionality available via PNC. In particular there was limited understanding of the implications of a ViSOR (Violent and Sexual Offenders) marker. The Force is therefore exposed to the risk that valuable intelligence could be lost in this area.

2.3.1.2 The lack of a formal communications strategy for the PNC has resulted in many officers learning about the system through 'word of mouth'. Whilst this method can produce positive results amongst close knit teams, it also carries a risk that messages become diluted and officers do not receive sufficient information. A lack of knowledge concerning the functionality of the PNC can lead to missed opportunities for the Force.

2.3.1.3 In previous inspections of other forces, HMIC Auditors have identified that good practice in this area is where the resources and advice of the Force Marketing Department has been sought. The presentations provided by PITO are another free resource open to WMP that could be harnessed to increase staff knowledge surrounding the intelligent searches that PNC can provide.

Recommendation 6

Her Majesty's Inspector of Constabulary recommends that the Force develops a coherent marketing strategy encompassing all the different methods of communication available to raise awareness of the PNC functionality amongst all staff.

2.3.2 PNC Training

2.3.2.1 Student Constable PNC training is limited to giving the student the skill to request a PNC check. Given the module format of this training, the Force is missing an opportunity to training the intelligence functionality in 'bite size' chunks through numerous stages of the training, rather than a one off session that is likely to have little impact.

2.3.2.2 PITO customer services regularly visit WMP to provide an input onto the detective constable and senior investigating officer courses.

2.3.2.3 There is not a comprehensive document that defines which roles within the organisation should be given access to the PNC. This can therefore

lead to an inconsistent approach to the allocation of PNC courses. In previous inspections this job classification document has been authorised by the PNC Strategy Group which gives it an objectivity and independence from other departments within the organisation.

2.3.2.4 The feedback from interviews indicated that the PNC training on offer was sufficient to meet the needs of the WMP. However, the feedback from operational staff was that courses are often difficult to obtain. Three out of the six OCUs visited reported problems in booking PNC courses within a reasonable time scale. Two of the OCUs were paying the trainers to provide PNC courses on overtime. Whilst it could be argued that this is an acceptable use of resources in the short term to overcome the demand peaks and troughs, the Force has to satisfy itself that there is not a more economical solution to the training provision.

2.3.2.5 Previous inspection work in other forces has shown that the availability of modular PNC courses has allowed them to focus resources to where they are needed. It has also enabled the Force concerned to reduce its abstraction costs as the courses are shorter.

2.3.2.6 HMIC Auditors are concerned over the length of mobile data terminal (MDT) training which is delivered over one day. Upon completion the officer is given access to perform basic PNC names and vehicle checks. HMIC would refer the Force to the national PNC training guidance issued by PICTTS (Police Information Communication Technology Training Service) which provides for a 4 day course on Names Enquiry.

2.3.2.7 There are similar concerns regarding the PNC element to the ICIS training course. The ICIS training is delivered over 5 days with one day allocated for the PNC input. PICTTS recommend minimum lengths of training courses depending on the PNC functionality that is covered. The Force needs to satisfy itself that it is adhering to the national guidelines for the MDT and the ICIS training courses.

2.3.2.8 On conclusion of training each candidate is asked to complete an end of course evaluation sheet to rate the course, its content, the training facilities and the trainer. However no post evaluation training is conducted, for example three months after the course, which would assist in the training design through an evaluation of whether the course provided the trainee with the correct tools and information back in the work place.

2.3.2.9 HMIC Auditors were informed that the Force is in the process of developing a computer based training package for PNC refresher training. This has been identified as good practice in previous inspections, WMP is therefore encouraged to continue with this development.

Recommendation 7

Her Majesty's Inspector of Constabulary recommends that the Force:

- **Satisfies itself that it is providing PNC courses in the most economical way.**
- **Reviews the MDT and ICIS courses to ensure that they adhere to the PICTTS Occupational Standards for PNC training.**
- **Introduces post training evaluation after trainees have had the opportunity to put the training into practice.**

2.4 Partnerships and Resources

2.4.1 Update of Court Results

2.4.1.1 The Force has developed a good meeting structure with the courts. The Local Criminal Justice Board is attended by the DCC. There are 8 Local Criminal Justice groups covering the 21 OCU areas. In addition there is a Courts Process and Enforcement Action Delivery Board attended by an Inspector from the central Criminal Justice Development Unit. The issues with the timeliness of the court registers were being progressed through this arrangement.

2.4.2 Non Police Prosecuting Agencies

2.4.2.1 Under national agreements police forces are responsible for updating the PNC with data from Non Police Prosecuting Agencies (NPPAs). In order to ensure that PNC records are complete, accurate and up to date forces need to introduce arrangements to ensure that all NPPA information is received in a timely manner and that the data received is of the quality expected from its own officers and staff.

2.4.2.2 HMIC were made aware that WMP have recently sent out letters to their main NPPAs reminding them of their responsibilities in respect of both the timely submission of data and the full amount of information required to update the PNC record.

2.4.3 Force Representation at National PNC Meetings

2.4.3.1 The Force is commended for permitting the PNC Liaison Officer to Chair the PNC East/West Midlands Regional Practitioner Group and attend the Names Working Party and the P4G so that the Force can gain the benefit of the national perspective and input into the decision making process for current and future developments of the PNC.

2.5 Processes

2.5.1 Compliance with the Codes of Practice

2.5.1.1 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). The Code stipulates that 90% of recordable offences be entered onto PNC within 24 hours of the commencement of proceedings. The commencement of proceedings is defined as when a person is arrested, reported or summonsed.

2.5.1.2 Unfortunately due to the limitations of the interface between ICIS and the PNC, WMP is unable to record all their records from the commencement of proceedings onto the PNC. DNA and fingerprints are taken when the offender is taken into custody for a recordable offence, but these details are not entered onto the PNC until a final disposal decision is made. Whilst HMIC Auditors are aware that other Forces have employed manual 'work arounds', it was reported that due to the volume of arrest summons reports processed each month and the subsequent effect on ICIS interface case resulting, WMP has taken the decision not to employ a manual work around, but to use the process as described above until the electronic solution is available.

2.5.2 Data Quality

2.5.2.1 HMIC Auditors carried out reality checks comparing the information on ICIS with the information contained on the PNC. Apart from the two issues discussed in the subsequent paragraphs overall there were only minor errors detected.

2.5.2.2 However, in 38% of the records checked it was noted that the 'Other Details' page in a names record had been populated with domestic details such as how much social security benefit the person is claiming. The instruction on the ICIS screen when the office is entering the information specifically states that domestic details are not to be submitted via this section. The officers are therefore not adhering to the instruction given on their own system. In addition, some of the details are out of date. There were two entries noted that dated back to 1996. To comply with the 1998 Data Protection Act principle WMP would need to ensure that the information is still current and delete any that no longer applies.

2.5.2.3 If WMP continues to input information onto this page it would have to manage the data to ensure that it is still accurate and up to date. This section in a PNC names record does not generate a 'Daily Activity File' print which would have enabled the Force to regularly check out of date information. The management of this information would therefore be a laborious manual process.

2.5.2.4 The second issue surrounded the transfer of information from ICIS to the PNC. It concerned the postcodes recorded against the offender's home address. It was noted during the reality checks that a Wolverhampton postcode was being recorded against a Birmingham address when it was transmitted from the ICIS application to the PNC. After discussions with the ICIS support team it was ascertained that it was a system fault occurring when the information was downloaded from ICIS to the PNC. The postcode is a field which is searchable using QUEST so it has implications for the accuracy of these searches.

2.5.2.5 HMIC Auditors were informed that the OCUs each check seven A/S records per week. The reality checks confirmed that this quality assurance (QA) process is effective as no inaccuracies in the data were detected in the 9 fields included in the QA process. The offenders home address is not one of the fields included in the QA process, so the interface problem was not detected. In order to improve the QA process WMP could consider changing one or more of the 9 fields in the QA process every 6 or 12 months to enable the force to regularly check more of the accuracy of the data on the PNC.

Recommendation 8

Her Majesty's Inspector of Constabulary recommends that the Force:

- **ensures that the data on the 'other details' page within a PNC names record adheres to the principles of the 1998 Data Protection Act and;**
- **an electronic solution is provided for the accurate exchange of information between ICIS and the PNC in the postcode recorded against an offender's home address.**

2.5.3 Bail Conditions

2.5.3.1 Currently WMP do not input bail conditions onto the PNC relying instead on their internal system. WMP is a policing area that is completely surrounded by other police forces. The current approach denies them access to this information which may have direct impact on future custody decisions.

Recommendation 9

Her Majesty's Inspector of Constabulary recommends that the Force review the decision not to input bail onto the PNC in light of the benefits it would bring to operational policing for the whole of the community.

2.5.4 MO Keywording

2.5.4.1 MO keywords are a parameter that can be used during a QUEST search. This is an important intelligence feature of the PNC, which can be used to identify possible suspects, particularly for serious offences, during a police investigation. It has been a requirement for several

years that all forces must input MO keywords into the system to ensure that searches via QUEST cover the whole of PNC. It is noted from the PITO statistics that the WMP cumulative total in this area puts the Force in the bottom quartile.

2.5.4.2 HMIC Auditors were informed during the inspection that WMP are in the process of addressing the issues surrounding the identification of cases to keyword. Currently, noteworthy cases are identified by the OCU criminal justice staff. It is proposed that the arresting officer will in the future identify those cases to keyword. This should enable the WMP to more efficiently identify the offences which will justify the keywording procedure. HMIC Auditors therefore encourage the Force to undertake this change to the process.

2.5.4.3 WMP is however commended for the thorough way in which they keyword the records already completed. It is vital however, to the success of PNC that the Force ensures the input of MO keywords for all these serious cases.

2.5.5 The Input of Disqualified Driver Reports

2.5.5.1 The input of disqualified driver reports is undertaken by the PNCB for the whole of the Force area. The original information is posted to the PNCB from the OCU court resulting units on paper cards. This obviously builds in a delay to the information being entered onto the PNC. The Force does operate an internal email system which would appear to be a more efficient and prompt method of exchanging the information.

Recommendation 10

Her Majesty's Inspector of Constabulary recommends that the Force review the effectiveness of its current process to input the disqualified driver reports.

2.5.6 Ad Hoc Intelligence Updates[1]

2.5.6.1 WMP captures ad hoc intelligence updates, for example a change of address or a new tattoo, on the local IMS application where the information is assessed and available via a FLINTS (the local intelligence system) query. However, there was not a robust process in place to ensure that this information is transferred to the PNC if it is suitable.

Recommendation 11

Her Majesty's Inspector of Constabulary recommends that the Force introduce a procedure to update the PNC with ad hoc intelligence recorded on the IMS intelligence application to improve the quality of the information on the system. Implementation of a formal procedure should be accompanied by sufficient marketing of the process.

[1] Information applicable for update to PNC that originates from a source other than the creation of an Arrest/ Summons report.

2.6 Results

2.6.1 In terms of Arrest/ Summons (A/S) updates WMP has seen an approximately 35% increase in the number of reports that the Force has to input on a monthly basis as a result of undertaking the full powers of the 2003 Criminal Justice Act. There is a concern however, that the trend in the number of days to enter 90% of A/S reports has continued to increase since the recording of CJ Arrestees was commenced. Prior to January 2005 the Force was achieving between 1 and 2 days, in October 2005 this figure had deteriorated to 63 days. However, HMIC Auditors were made aware of imminent changes to the ICIS custody application that should allow the Force to return to its previous good performance.

2.6.2 WMP's performance in the area of court resulting has plateaued approximately 5% below the 75% target. The ACPO PNC Code of Practice does state that forces have 7days from the receipt of the court registers to input the data onto the PNC. The national statistics produced by PITO do not allow that figure to be recorded. HMIC Auditors are therefore reliant on the Force providing the evidence if the PITO statistics indicate that they are above the 10 day target. The evidence provided by the force is not comprehensive – some of the OCU court resulting sections have not provided data, making comparisons difficult. The evidence from focus groups and interviews was that the OCUs did not have a standardised format in which to gather this information, some were still recording it in a paper format making overall calculations laborious. Collation of comprehensive management information would also enable the Force to escalate issues with the provision of the court registers within three working days for the courts through the LCJGs and LCJBs when necessary.

Recommendation 12

Her Majesty's Inspector of Constabulary recommends that the Force standardises and electronically records its monthly data collection from the Criminal Justice or Glidewell Units concerning the receipt of the court registers and the subsequent recording onto the PNC.

2.6.3 With regard to outstanding impending prosecutions (IPs), these have remained relatively static throughout the 12 months back to November 2004. HMIC Auditors are aware that the Force has worked hard over the previous 2 years to reduce their outstanding IPs to their current level. WMP is the second largest police force in England and Wales yet there are 6 police forces with more outstanding IPs. The Force is commended for their management of its outstanding IPs.

APPENDIX A

SUMMARY OF RECOMMENDATIONS FOR WEST MIDLANDS POLICE

Recommendation 1

Her Majesty's Inspector of Constabulary recommends that the Force recommends that the Force ensures that the Data Managers meetings, the Ops Centre Managers meetings, the CSB managers meetings and the ICIS User Group include PNC as a standing agenda item to ensure that there is an interaction between them and the PNC Strategy Group.

Recommendation 2

Her Majesty's Inspector of Constabulary recommends that the Force ensure that there is compliance in the OCUs to the PNC policy documents.

Recommendation 3

Her Majesty's Inspector of Constabulary recommends that WMP introduces an independent audit, at least annually, of all user access administration.

Recommendation 4

Her Majesty's Inspector of Constabulary recommends that the Force recommences the process of PNC transaction monitoring in line with the ACPO Data Protection Audit Manual.

Recommendation 5

Her Majesty's Inspector of Constabulary recommends that the Force ensures that it undertakes sufficient auditing to comply with the PNC Code of Connectivity whilst it is embedding the Quality Improvement Process.

Recommendation 6

Her Majesty's Inspector of Constabulary recommends that the Force develops a coherent marketing strategy encompassing all the different methods of communication available to raise awareness of the PNC functionality amongst all staff.

Recommendation 7

Her Majesty's Inspector of Constabulary recommends that the Force:

- Satisfies itself that it is providing PNC courses in the most economical way.
- Reviews the MDT and ICIS training courses to ensure that they adhere to the PICTTS Occupational Standards for PNC training.
- Introduces post training evaluation after trainees have had the opportunity to put the training into practice.

Recommendation 8

Her Majesty's Inspector of Constabulary recommends that the Force :

- Ensures that the data on the 'other details' page within a PNC names record adheres to the principles of the 1998 Data Protection Act and;
- An electronic solution is provided for the accurate exchange of information between ICIS and the PNC in the postcode recorded against an offender's home address.

Recommendation 9

Her Majesty's Inspector of Constabulary recommends that the Force review the decision not to input bail onto the PNC in the light of the benefits it would bring to operational policing for the whole of the community.

Recommendation 10

Her Majesty's Inspector of Constabulary recommends that the Force review the effectiveness of its current process to input the disqualified driver reports.

Recommendation 11

Her Majesty's Inspector of Constabulary recommends that the Force introduce a procedure to update the PNC with ad hoc intelligence recorded on the IMS intelligence application to improve the quality of the information on the system. Implementation of a formal procedure should be accompanied by sufficient marketing of the process.

Recommendation 12

Her Majesty's Inspector of Constabulary recommends that the Force standardises and electronically records its monthly data collection from the Criminal Justice or Glidewell Units concerning the receipt of the court registers and the subsequent recording onto the PNC.

APPENDIX B

SUMMARY OF GOOD PRACTICES AT WEST MIDLANDS POLICE

- The monthly performance statistics are produced so that each OCU are able to determine their own individual performance.
- The Force has a strategic Action Plan which is viewed as a working document.
- There is a comprehensive set of policy documents available on the Force intranet.
- The Information Security policy is reviewed annually.
- The sending of letters to the main NPPAs who provide data to the PNC via the WMP.
- Enabling the PNC Liaison Officer to chair the East/West Midlands Regional Practitioner Group and attend the national Names Working Party and the P4G.

APPENDIX C – 'ON THE RECORD'

THEMATIC INSPECTION REPORT ON POLICE CRIME RECORDING, THE POLICE NATIONAL COMPUTER AND PHOENIX INTELLIGENCE SYSTEM DATA QUALITY - RECOMMENDATIONS

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 – 1ST PNC REPORT

POLICE NATIONAL CONPUTER DATA QUALITY AND TIMELINESS – RECOMMENDATIONS

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 – 2ND PNC REPORT

POLICE NATIONAL COMPUTER DATA QUALITY AND TIMELINESS – RECOMMENDATIONS

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.