WEST MERCIA CONSTABULARY

12 - 16 DECEMBER 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 Mercia Constabulary (WMC) between 12th and 16th December 2005.

1.1.2 The Constabulary was subject to a PNC Compliance Audit using the 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 her 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 2 of the 5 Borough Command Units (referred to as 'Divisions'). 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 Mercia Constabulary is responsible for policing the counties of Shropshire and Worcestershire and the unitary authorities of Hereford, Telford and the Wrekin. It serves a resident population of about 1.16 million, 2.3% of whom are of minority ethnic origin. The force covers 2,868 square miles and is the fourth largest geographic policing area in England and Wales.

1.2.2 The five divisions and their respective policing challenges are diverse, both demographically and geographically. They include the densely populated urban conurbation on the edge of Birmingham, together with city areas such as Worcester, and sparsely populated rural areas in the remainder of the Force area.

1.2.3 The Constabulary headquarters, Hindlip Hall, is a 40 acre country estate, at the centre of which is a Grade II listed Georgian manor house which is situated about four miles north of Worcester. The command team comprises the Chief Constable, who joined the Force in August 2003, a Deputy Chief Constable (DCC) and two Assistant Chief Constables (ACCs) responsible for territorial operations and specialist operations. There are also two police staff Directors, one being responsible for administration and finance, whilst the other holds a portfolio encompassing organisation and strategy. West Mercia employs 2,400 police officers, 1650 police staff, 300 Special Constables and 80 community support officers.

1.2.4 The creation of Arrest/ Summons records at West Mercia is a semi-automatic process which requires the custody officer to update the Force custody system known as CRIMES (Crime Recording Information Management System) with partial details required to create a record on the PNC. This is followed by the arresting officer completing a manual source input document (known locally as the 'CO 11') which contains all

the data required for a complete record on the PNC. This is posted to the PNC Bureau (PNCB) along with the DNA and fingerprint samples, who will then complete the record on the system.

1.2.5 The PNCB also update the PNC with wanted missing reports, disqualified driver reports, warning signals, information and intelligence markers and vehicle and property reports. In addition it performs a 24/7 service to the Force for enhanced searches on the system such as Vehicles On Line Descriptive Searches (VODS) and Queries Using Extended Search Techniques (QUEST).

1.2.6 The CJU (Criminal Justice Unit) staff based within the divisions update the court results onto the CRIMES application which then transfers them to the PNC. The magistrates court disposals are printed from the Lord Chancellor's Information System (LCIS) terminals based in each CJU. The Force does not update court adjournment details onto the PNC. The LCIS terminals cannot be used to research outstanding court results.

1.2.7 The CJUs receive the Crown Court results via the Xhibit application. Unfortunately the system does not supply details of indictments so the Force has to wait until these are faxed through from the crown court in order to update the PNC record. However, the Force has always received these disposals more quickly than those from the magistrates' courts.

1.3 Methodology

1.3.1 A full inspection against the 2005 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:

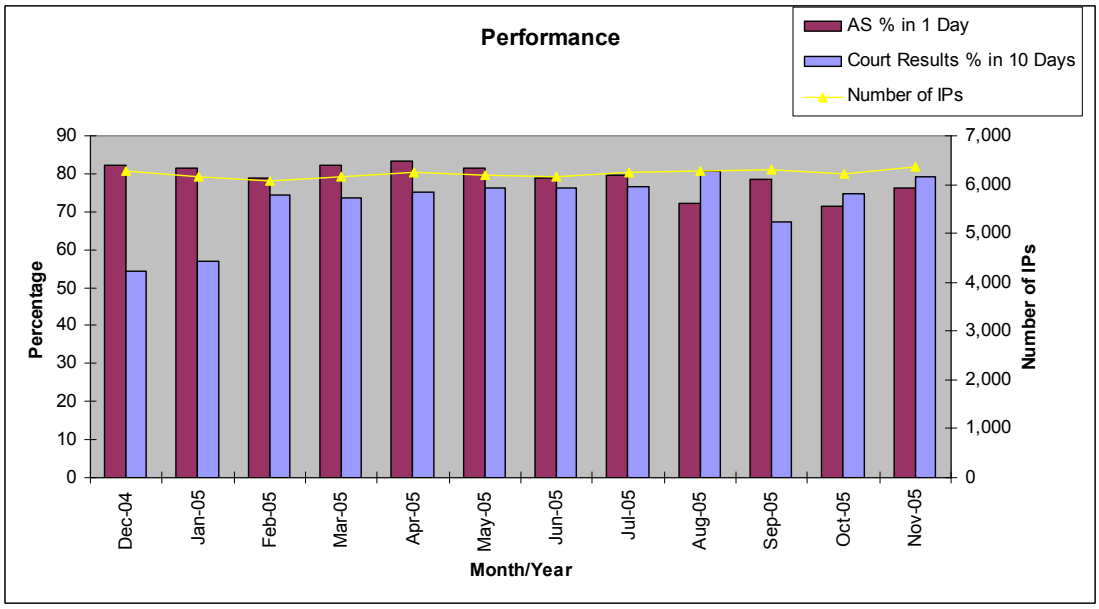
- 90% of recordable offences entered onto PNC within 24 hours of the commencement of proceedings. The commencement of proceedings being defined as when a person is arrested, reported or summonsed.
- 50% of all finalisations being entered onto PNC within 7 days of the information being received by the police. This target increased to 75% on 1 July 2005, six months after the commencement of the Code. (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 November 2005, West Mercia input 76.3% of Arrest/ Summons (A/S) updates on PNC within 24 hours. This shows a slight decline in performance over the previous 6 months from 81.3% in May 2005. It should be noted that the force has not achieved the target of 90% in any of the 12 months to November 2005.

1.4.5 West Mercia's performance in terms of court results has shown improvement against the Code of Practice target. In December 2004 the Force entered 54.4% of results within 7 days of the court date. This has increased to 79.2% being entered within 10 days in November 2005. There has only been one month (September 2005 – 67.2%) when the Force appeared from the PITO statistics not to have achieved the target in the Code of Practice in this area of activity.

1.4.6 In terms of Impending Prosecutions (IPs) West Mercia has shown a slight increase of 1% in the 12 months to November 2005. Whilst this shows that the Force is effectively managing its outstanding cases on the PNC, comment should be made that the figure would have substantially increased if the Force was complying with the Code of Practice by updating all records at the point of arrest.

1.4.7 A graph illustrating West Mercia's performance in the 12 months to November 2005 is shown below:[1]



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] Key: Purple columns indicate A/S performance, blue show court results performance and the yellow line shows the increase/ decrease in Impending Prosecutions.

1.5.2 This assessment is based on the detailed findings of the report which highlight concerns in some areas of activity. In particular, the Force needs to implement procedures which will ensure that it consistently achieves the PNC Code of Practice target in respect of the input of arrest summons within 24hours. In addition, the Force should ensure that there is sufficient data protection auditing undertaken to reduce the risk of inaccurate data on the PNC and that it satisfies itself that there is sufficient resilience in the training department to meet the current and future demands.

1.5.4 The findings of this report should 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*

1.5.5 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 PNC Steering Group

2.1.1.1 At the time of inspection, West Mercia Constabulary (WMC) had recently reorganised the portfolios of the DCC and the ACC (Operations) so there are now two chief officers with responsibility for the PNC within their remit. Whilst in pervious inspections in other forces this has not been an ideal situation and has lead to fragmented ownership, it was a new change within the management structure of WMC and has yet to embed into the culture. HMIC Auditors were reassured as the performance against the targets can be split between the two chief officers so each can be held accountable for their individual areas of responsibility.

2.1.1.2 West Mercia Constabulary (WMC) has a PNC Steering Group which meets on a quarterly basis and is chaired by the Deputy Chief Constable. Stakeholders from across the force are invited to attend the meetings although a review of the minutes showed that there is currently no representation invited from the Communication environment. As officers and staff in this area are likely to be the heaviest users of the system, HMIC Auditors believe that they should be represented at a strategic level. The review also highlighted the fact that whist divisional representatives are invited to the meetings, there is rarely any representative in attendance. This could lead to a breakdown in communications beyond the headquarters environment and may be, in part, responsible for some of the issues discussed later in this report.

Recommendation 1

Her Majesty's Inspector of Constabulary recommends that the Force include a representative from the communications environment to attend the Steering Group and urges divisional representation to attend the meeting on a regular basis.

2.1.2 Responsibility and Accountability

2.1.2.1 Monthly management information is produced outlining the performance of each Division in terms of the timeliness of data submission. Whilst this is circulated at the monthly Force Performance Group of Divisional Commanders it has not featured as an item for discussion in recent months. HMIC Auditors were made aware that this situation was about to change as the DCC is going to raise the profile of PNC issues to ensure that the concerns regarding the arrest summons performance can be discussed at a strategic level. HMIC Auditors see this as a positive step and therefore encourage the Force to undertake this change.

2.1.2.2 Further good practice was identified within the PNCB where dip sampling takes place of PNC updates. The Corporate Data Quality Unit (CDQU) quality check the work of the PNCB staff and record the results of these checks. This is viewed as good practice.

2.2 Policy & Strategy

2.2.1 PNC Policy and Strategy

2.2.1.1 In HMIC's Second Report on the PNC Data Quality and Timeliness (the recommendations of which are provided in Appendix E of this report), it was recommended that a PNC Strategy should be an integral part of a force's information management strategy. However, whilst the WMC document provided to the HMIC Auditors identified the issues surrounding the published HMIC PNC protocols, it did not consider any future developments in the functionality and use of the PNC.

2.2.1.2 In particular, the introduction of the National Firearms Licensing Management System and the introduction of the NSPIS Custody and Case Preparation applications which will impinge on the operation of the PNC. There will also be training and auditing issues which the Force would need to take into account. The document would therefore enable the Force to take a more proactive approach to the PNC developments.

2.2.1.3 WMC has some documented policies with regard to PNC usage which are publicised on the Force Intranet. However, the anecdotal evidence from interviews and the focus groups was that some staff were not aware of their responsibilities as far as PNC is concerned. In addition, the Force has recently commenced the recording of DNA and fingerprints on arrest, but there was not a document to cover the new procedure which has resulted in the divisions writing and adopting their own. Therefore, the Force risks having different policies and procedures being implemented in each of its five divisions.

Recommendation 2

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

- **Expands the current PNC strategy document to include future changes to the PNC to enable it to prepare a strategic position to the forthcoming developments and to respond effectively at an operational level when these changes are introduced**
- **Ensures that it produces and publicises a comprehensive set of policy documents for the update and use of the PNC.**

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 Information Security and Data Protection training. Some good practices and some areas of concern were identified during the review and these are discussed further below.

2.2.2.2 Access to the PNC is managed by the Training unit. The Force has processes in place to ensure that a user is only given access to the system upon completion of a training course. There are also processes in place to ensure that leavers have their access to the system removed. However, this process could be improved by ensuring that those officers and staff who's job changes and no longer need access to the PNC, those on long term sickness absence and any suspended officers and staff have their PNC access amended or revoked as necessary.

2.2.2.3 Whilst HMIC Auditors do not question the integrity of the Trainers, there is some risk to the organisation in having individuals able to make such changes to system access with no independent auditing of the activity being carried out. In addition, as this is an administrative function it is questionable whether this is an efficient use of a trainer's time.

Recommendation 3

Her Majesty's Inspector of Constabulary recommends that WMC:

- **Introduces a process to ensure that officers and staff who change job roles, are on long term sick leave or who are suspended have their access amended or removed from the system as appropriate;**
- **Introduces an independent audit, at least annually, of all user access administration.**

2.2.2.4 HMIC Auditors were informed that WMC use of the 'Easy i' online computer based training package for their data protection training. Staff are required to attain 100% in the assessment. This is viewed as good practice.

2.2.2.5 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. At WMC this is a function of the Information Compliance Unit who use random number generator database package to select ten transactions daily for verification. A form is sent to the individual who requested the check to confirm that it was conducted for operational policing purposes and supporting documentation is requested. The form is signed off by the individual's supervisor before being returned

2.2.2.6 Any unacceptable replies are returned to the appropriate manger. All transaction fields are checked for quality and any errors found are classified and documented. Abuse of the system would be reported to the Professional Standards Department. HMIC Auditors encourage WMC to continue with this current level of transaction monitoring.

2.2.2.7 Data Protection Audits are the responsibility of the Information Compliance Manager at WMC. There is no annual risk assessment of its IT data systems undertaken. The last audit undertaken was in October and November 2003 of the WMC outstanding warrants. Two of the recommendations in that report reiterated practices already taking place within WMC, two of the recommendation contradicted each other and there was no evidence provided during the inspection that changes to processes had been made as a result of the findings.

2.2.2.8 The PNC Code of Connectivity mandates the requirement for PNC audits in accordance with Section 2 of the ACPO Manual for Data Protection Management. In addition, in the current climate post Bichard Inquiry, it is imperative that forces ensure that data protection issues can be identified and rectified as a matter of priority. HMIC Auditors believe that making the PNC Steering Group responsible for ensuring that audit recommendations are implemented forcewide would improve on the current process by guaranteeing a corporate approach and introducing an additional level of accountability.

Recommendation 4

Her Majesty's Inspector of Constabulary recommends that the Force urgently review the situation within the Data Protection Unit to enable formal data protection audits to be conducted against the PNC data.

2.2.2.9 HMIC Auditors also reviewed the role of the Professional Standards Department (PSD) with regard to PNC issues at WMC. The PSD is independent of operational activities and such independence is viewed as good practice. In addition, the Information Compliance Manager has

strong links with the PSD which ensures that the PSD is notified of any breaches of system security. The inclusion of PNC trained operators in the PSD would enable them to independently conduct investigations involving PNC activity and to be proactive in the investigation of system misuse and abuse.

Recommendation 5

Her Majesty's Inspector of Constabulary recommends that the Force considers the introduction of a PNC capability within the PSD environment.

2.2.2.10 Finally with regard to PNC system security, HMIC Auditors reviewed the Information Security Policy. Whilst it is seen as good practice to have a security policy specifically applicable to the PNC, the policy was at the time of the inspection still in a draft format. It was also the opinion of the HMIC Auditors that there are areas of the policy which could be open to challenge in a disciplinary situation. For example the policy states that "All phone call received on an outside line will be subject to ring back unless:
The person is known to the operator".
This is a subjective statement and would be difficult to prove that the PNC operator did not know the person requesting the PNC check from an outside line.
WMC is advised to amend the policy to ensure that the policy is not open to interpretation.

Recommendation 6

Her Majesty's Inspector of Constabulary recommends that the Force reviews and amends the PNC System Security Policy prior to it being ratified and published.

2.3 People

2.3.1 Marketing and Awareness

2.3.1.1 During meetings and focus groups, HMIC Auditors noted variable levels of awareness among officers and staff of the PNC functionality as an aid to operational policing. In particular, knowledge of QUEST was low. An example of the low level of knowledge was a discussion regarding the new MOT information stored on the PNC. One officer reported that he only found about this change when he took his own car for an MOT, he had not received any information within force. HMIC Auditors were also concerned that police officers and staff were generally unaware of ViSOR (Violent and Sexual Offenders Database). The Force is therefore exposed to the risk that valuable intelligence could be lost in this area.

2.3.1.2 It was pleasing to note however, that officers and staff were aware of the restrictions surrounding the use of driving licence and insurance information and are therefore unlikely to be utilising this data inappropriately.

2.3.1.3 However, the Force relies heavily on its intranet for communication, thus placing a reliance on officers and staff to find information for themselves. It is the view of HMIC Auditors that a focused marketing campaign should be carried out to raise the level of awareness of PNC functionality, covering a variety of communications methods across the Force. This campaign should be developed as part of a marketing strategy owned by the PNC Steering Group but using expert resources such as that of the force marketing department or the services of the PITO (Police Information Technology Organisation) PNC Customer Services team.

Recommendation 7

Her Majesty's Inspector of Constabulary recommends that the Force publishes and implements a Communication Strategy to raise awareness for the effective use of PNC across the Force.

2.3.2 PNC Training

2.3.2.1 PNC training was a further area at WMC where HMIC Auditors identified both good practice and areas of concern. The Force has currently two accredited PNC trainers, who also have responsibility for training other IT systems. The PNC courses are provided on a modular basis which is seen as good practice. In addition, an audit trail is kept of the changes made to the PNC courses so that the Force can ascertain for any student the functionality that was being delivered at that point in time. The PNC trainers are assessed annually by the training and development officer. The trainers are given positive feedback as well as areas for development. These are both seen as good practice.

2.3.2.2 However, there were concerns raised with regard to training availability and prioritisation. At the time of the inspection, the Force had a backlog for the delivery of PNC enquiry courses,

2.3.2.3 HMIC Auditors also noted that it was the responsibility of each Division to nominate individuals for PNC training. Once the bids are in, the volumes are reviewed by the Divisional Training Panels which then determines the staff who are eligible for training courses. The Force uses the Integrated Competency Framework to assess skill requirements which do not take into account IT role profile. As a result, officers who had requested PNC training and required it as a core part of their role, are still waiting for training, these include staff who update the PNC. This is a situation which the Force needs to address if officers and staff are to be able to perform their duties effectively.

2.3.2.4 The Force had already good practices in ensuring that all course attendees are subject to a formal assessment prior to being given access to the PNC and the course content included data protection and information security issues throughout.

2.3.2.5 The final point to be made in respect of PNC training is post training evaluation. The Force has some good practices in place with a “Happy Sheet” at the end of each course. In addition, the Force is also using the Kirkpatrick Evaluation Model which is an internationally recognised framework for monitoring the effectiveness of training courses. Unfortunately, there was no evidence from interviews and focus groups that this was being used to monitor PNC training.

Recommendation 8

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

- **Considers options available to provide resilience to the current PNC training arrangements to ensure that training needs can be met;**
- **Reviews its process for prioritisation of places for courses to ensure that those who require PNC in exercise of their daily duties receive training at the earliest opportunity;**
- **Expand the Kirkpatrick Training Evaluation Model to include all PNC courses.**

2.4 Partnerships and Resources

2.4.1 Relationship with the courts

2.4.1.1 The Force has a good liaison with its local courts through informal meetings and the Local Criminal Justice Board (LCJB). The criminal justice superintendent attends the performance delivery group and takes issues with the late delivery of magistrates' courts registers. If this cannot be resolved through this informal mechanism the concerns can be taken to the LCJB. The Force is encouraged to continue to liaise with the courts through the LCJB in order to influence the provision of court registers in a timely manner.

2.4.2 Relationship with non police prosecuting agencies (NPPAs)

2.4.2.1 With the introduction of the Code of Practice for PNC in January 2005, the target for the input of A/S records no longer includes those records which are updated as a result of an NPPA prosecution. However, there is still a need for forces to ensure that these records are updated in a timely manner to assist operational policing activity. This can only be achieved if forces encourage the NPPAs to provide complete, timely and accurate information for input to PNC. HMIC Auditors would therefore encourage the Force to introduce Service Level Agreements with its NPPAs to achieve this.

2.5 Processes

2.5.1 Creation and update of Arrest/ Summons (A/S) reports

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 (NCPE) 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 The 2003 Criminal Justice Act enabled forces to obtain DNA and fingerprints when the offender is arrested for a recordable offence. An arrest summons report has to be created on the PNC for the DNA and fingerprints to be retained on the national database. The act allowed this change in procedures from April 2004. WMC employ a custody application (CRIMES) which transfers the data to the PNC to create the arrest summons report. Unfortunately due to the limitations of the interface between CRIMES and the PNC, the Force has been unable until recently to record the DNA and fingerprints onto the PNC on arrest using Crimes. The Force has therefore lost the opportunity to gather and record potential forensic evidence on the national database for 18 months.

2.5.1.3 WMC introduced a manual 'workaround' in one of its custody units in June 2005. An electronic solution was created within CRIMES to permit the Force to record DNA and fingerprints on arrest throughout all the Divisions. It was reported that this solution became available from 7th December 2005.

2.5.1.4 The Force does not have a policy to support this change in the procedure, as referred to in paragraph 2.2.1.3. HMIC Auditors are not reassured that the Force has adopted this change throughout all its Divisions. Statistics produced after the inspections show that between November and January WMC only increased the number of A/S reports processed each month by 0.3%. Previous inspections in other forces have shown that when the powers of the 2003 Criminal Justice Act have been fully embraced, forces have experienced an increase of between 40% and 60%. This data is available within the monthly statistics produced by PITO.

2.5.1.5 Finally under this section, it was reported that some records fail to transfer from CRIMES to the PNC; CRIMES generates 'reject messages' to alert the Force. The records can be manually released, but at the time of the inspection this was not being undertaken out of hours and at the weekends. The PNCB operate 24/7 but currently are not trained to carry out this function. Providing a 24/7 to deal with the 'reject messages' would enable the Force to ensure that all records that were processed through the CRIMES application reached PNC within the 24 hour timescale.

Recommendation 9

Her Majesty's Inspector of Constabulary recommends that the Force reviews its processes for the update of A/S records, to ensure that all PNC records are complete, accurate, timely, and that the force complies with the Code of Practice.

2.5.2 Non – custody cases

2.5.2.1 During the inspection HMIC Auditors reviewed the process for PNC updates for cases that do not pass through custody, e.g. individuals reported for summons or issued with a Fixed Penalty Notice for a recordable offence. Under the Code of Practice for PNC the case should be updated within 24 hours of the commencement of proceedings and, as such, these cases are included within the Code. On 1st November 2005 WMC introduced a new procedure for PNDs. The police officers can now phone through the details to the Central Crime Recording Unit who input the information onto CRIMES. As this process has yet to embed into the culture at WMC, the Force is advised to monitor the procedure to ensure that there is adherence to the change.

2.5.5 Ad hoc intelligence updates[2]

2.5.5.1 In WMC staff are expected to submit a NIR (National Intelligence Report) of any descriptive changes to individuals as a result of a PNC check being conducted outside of the custody unit. The NIR is forwarded to the Divisional Intelligence Unit who will enter it onto CRIMES and send it onto the PNCB to ensure that all PNC records are kept complete, accurate and up to date.

2.5.5.2 Staff were reminded of this process by a circulation in Force Orders on 12th March 2005. This circulation was prompted by an inspection into intelligence recording on West Mercia systems. However, whilst this is seen as commendable, regular reminders to staff of this process through a communications strategy (see recommendation 7) would reinforce the procedure.

2.5.5.3 A similar procedure is employed for intelligence updates to ViSOR (Violent and Sexual Offenders Register). When the system is updated by the divisional staff a NIR is completed and sent onto the PNCB for them to update the PNC with the relevant details.

2.5.6 Data quality

2.5.6.1 HMIC Auditors conducted reality checks at WMC to determine the quality of data being supplied by officers and subsequently input to PNC. This was achieved by obtaining a sample of source input documents (form CO 11), reviewing their content and comparing the details submitted to the PNC record. HMIC Auditors were pleased to note no major errors were identified.

2.5.6.2 The reality checks did expose an issue with the offence location correctly recorded on the CRIMES application but not transferring to the PNC. Of PNC records checked 36% did not contain an offence location whilst the CRIMES application did. Initial research indicated that the problem could occur when the offence location was updated, either

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

prior to the initial transfer to the PNC from CRIMES or after a subsequent update. However, due to time restrictions of the inspection the issue was not completely resolved.

Recommendation 10

Her Majesty's Inspector of Constabulary recommends that the Force explores the reasons for the difference between the offence location recorded on CRIMES and on PNC, so that either a manual or electronic solution can be found.

2.5.6.3 The Corporate Data Quality Unit (CDQU) quality assures the work of the A/S report updaters and the CJSU staff who update the court results onto CRIMES and subsequently PNC. Any errors identified are recorded for use in the appraisal system if appropriate.

2.5.6.4 The team supervisors in the PNCB are in the process of developing competency based training plans based for the staff to ensure that they are fully multi skilled. HMIC Auditors view both of these processes as good practice.

2.5.6.5 It was reported that although court remanded and adjournments are updated onto CRIMES these do not transfer to the PNC, so therefore remain on the local system. An area for improvement for WMC would be to update all court data onto the PNC which is also a requirement of the PNC Manual.

2.5.7 MO Keywording

2.5.7.1 MO keywords are a parameter that can be used during a QUEST search. This is an important feature of the PNC, which can be used to identify possible suspects, particularly for serious offences. It has been a requirement for several years that all forces must input MO keywords into the system to ensure searches via QUEST cover the whole of PNC

2.5.7.2 WMC is commended for the thorough way in which they keyword the records already completed. The records identified as a result of the reality checks supported this.

2.6 Results

2.6.1 In November 2005, WMC input 76.3% of Arrest/ Summons (A/S) updates on PNC within 24 hours. The Force has not achieved the ACPO Code of Practice target for the pervious 12 months and is currently in the bottom quartile. This is a concern for the HMIC Auditors.

2.6.2 However, WMC's performance in terms of court resulting is a much more positive and consistent achievement. Apart from one month out of the previous 12, the Force has consistently achieved the performance target as set out in the Code of Practice for PNC.

2.6.3 Finally, with regard to outstanding prosecutions on the PNC in the 12 months to November 2005 the Force has neither increased nor decreased. In April 2001, HMIC supported by the Home Secretary stated that all forces should be in a position to confirm that any outstanding case that is over twelve months old is legitimately outstanding. HMIC Auditors are therefore assured that the Force is able to provide such confirmation. However, it was reported during the inspection that the CJSUs reviewed the outstanding IPs every 6 months. Concentrating this work does however have a detrimental effect on the court resulting statistics as old court results are researched and updated. It also adds pressure onto the court staff every 6 months to investigate old outstanding court disposals. HMIC Auditors are aware in previous inspections that other forces undertake this work monthly. This is seen as good practice as it reduces the effect on the court resulting performance and it enables the court staff to regularly deal with the research required.

Recommendation 11

Her Majesty's Inspector of Constabulary recommends that the Force considers monthly research into their outstanding impending prosecutions.

APPENDIX A

SUMMARY OF RECOMMENDATIONS FOR WEST MERCIA CONSTABULARY

Recommendation 1

Her Majesty's Inspector of Constabulary recommends that the Force include a representative from the communications environment to attend the Steering Group and urges divisional representation to attend the meeting on a regular basis.

Recommendation 2

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

- Expands the current strategy document to include future changes to the PNC to enable it to prepare a strategic position to the forthcoming developments and respond effectively at an operational level when changes are introduced;

- Ensures that it produces and publicises a comprehensive set of policy documents for the update and use of the PNC.

Recommendation 3

Her Majesty's Inspector of Constabulary recommends that WMC:

- Introduces a process to ensure that officers and staff who change job roles are on long term sick leave or who are suspended have their access amended or removed from the system as appropriate;

- Introduces an independent audit, at least annually, of all users access administration.

Recommendation 4

Her Majesty's Inspector of Constabulary recommends that the Force urgently review the situation within the Data Protection Unit to enable formal data protection audits to be conducted against the PNC data.

Recommendation 5

Her Majesty's Inspector of Constabulary recommends that the Force considers the introduction of a PNC capability within the PSD environment.

Recommendation 6

Her Majesty's Inspector of Constabulary recommends that the Force reviews and amends the PNC System Security Policy prior to it being ratified and published.

Recommendation 7

Her Majesty's Inspector of Constabulary recommends that the Force publishes and implements a Communications Strategy to raise awareness for the effective use of PNC across the Force.

Recommendation 8

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

- Considers options available to provide resilience to the current PNC training arrangements to ensure that training needs can be met;

- Reviews its process for prioritisation of places for courses to ensure that those who require PNC in exercise of their daily duties receive training at the earliest opportunity;

- Expand the Kirkpatrick Training Evaluation Model to include all PNC courses.

Recommendation 9

Her Majesty's Inspector of Constabulary recommends that the Force reviews its processes for the update of A/S records, to ensure that all PNC records are complete, accurate, timely and that the Force complies with the Code of Practice.

Recommendation 10

Her Majesty's Inspector of Constabulary recommends that the Force explores the reasons for the difference between the offence location recorded on CRIMES and on PNC, so that either a manual or electronic solution can be found.

Recommendation 11

Her Majesty's Inspector of Constabulary encourages the Force considers monthly research into their outstanding impending prosecutions.

APPENDIX B

SUMMARY OF GOOD PRACTICE AT WEST MERCIA CONSTABULARY

- The production and circulation of management information at Divisional level on the timeliness of the submission of the arrest summons data.
- The dip sampling of PNC updates that are undertaken and recorded by the supervisors within the Corporate Data Quality Unit
- The use of the CBT package to refresh and reinforce Data Protection issues.
- The PSD is independent of operational activities.
- Audit trail for changes made to the PNC training courses.
- Annual assessment of PNC trainers.
- Thorough MO keywording of PNC names records.

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.