NORTHAMPTONSHIRE POLICE

19 – 22 FEBRUARY 2007

POLICE NATIONAL COMPUTER

COMPLIANCE REPORT

Report Contents

1. Executive Summary

1.1 Introduction

1.1.1 Her Majesty's Inspector of Constabulary (HMIC) conducted a Police National Computer (PNC) Compliance Inspection of Northamptonshire Police between 19 and 22 February 2007.

1.1.2 Northamptonshire Police was subject to a PNC Compliance Audit using the July 2005 Protocols on PNC compliance. Her Majesty's Inspector would like to acknowledge the Force for its services and also to place on record his thanks to all members of staff who contributed to this report and provided assistance during the inspection. Particular note is made of the comprehensive documentation that was provided to HMIC PNC Compliance Auditors (hereafter referred to as HMIC Auditors) in advance of 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 both of the Basic Command Units (BCUs) within the force. These views have been supported by reality checks conducted by HMIC Auditors.

1.2 Background

1.2.1 Northamptonshire Police covers an area of approximately 914 square miles and is located in the south of the East Midlands region. Local policing is managed at two BCUs (known locally as Areas) at Northamptonshire West and Northamptonshire North. The administrative centre of the county is Northampton with other main towns including Brackley, Corby, Daventry, Kettering, Rushden, Towcester and Wellingborough. The resident population is approximately 642,000.

1.2.2 The Force is headed by the Force Command Team, led by the Chief Constable, supported by the Deputy Chief Constable (DCC) and two Assistant Chief Constables (ACCs), with individual responsibilities for Operations and Support. There is also a Director of Resources who has responsibility for Finance, Administration and Property Services. The Force strength comprises approximately 1,327 full-time equivalent police officers, 1,176 police staff, 219 Special Constables and 129 Police Community Support Officers (PCSO).

1.2.3 The PNC function falls within the portfolio of the Deputy Chief Constable under the heading of Crime & Community. However, day to day management of the function is devolved to a Superintendent as Director of Intelligence and a manager of the PNC Bureau (Crime Intelligence). The PNCB manager, who also carries out the role of PNC Liaison Officer, is responsible for the staff who monitor the creation of arrest/summons reports, update court results, operational updates to the vehicles and names applications and vetting & disclosure.

1.2.4 The PNCB is based at the force headquarters and comprises approximately 25 staff. The PNCB is operational six days a week, operating alternating shift patterns in order to cover the hours between 7am and Midnight Monday to Friday and 7am to 6pm on Saturdays. The PNCB is closed on Sunday and Bank Holidays.

1.2.5 The PNCB is responsible for all updating to the names application throughout the force, including the monitoring of the timeliness and quality of transmissions between the NSPIS Custody application and the PNC. The PNCB also has responsibility for the creation of all A/S report for non-custody cases (e.g. Summons), magistrates and crown court results, bail conditions, MO keywords, wanted/missing, disqualified driver updates and quality control.

1.2.6 An arrest/summons report is created on the PNC via electronic transfer of data from the NSPIS Custody application. Staff in the PNCB monitor the transmission log to ensure that transmissions are successful and also to correct and re-transmit any transmissions that have failed. The transmissions create a full record on the PNC and the PNCB have an additional responsibility to ensure that records are of sufficient quality.

1.2.7 Court results are sent direct to the PNCB via an interface between the courts system (Equis) and the force. The force has the ability to print court registers from Equis once the information on Equis has been validated by the courts. Staff in the PNCB update court disposals directly onto PNC. Crown court results are received electronically via the Xhibit portal, with indictments being faxed through to the PNCB from the crown courts. PNCB staff monitor the exhibit system to retrieve results and match them to faxed indictments before they are manually updated onto the PNC.

1.2.8 VODS (Vehicle On-line Descriptive Searches) and QUEST (Queries Using Enhanced Search Techniques) searches are also provided by PNCB. The PNCB operates as a central point of contact for the whole force during the hours they are open. Out of normal hours, the Force Communication Centre (FCC) takes responsibility for urgent operational enquiries, including operational updates that may be required, for example, Stolen Vehicles or Wanted/Missing nominals.

1.3 Methodology

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

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

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

1.3.3 The first stage of the inspection involved the force providing HMIC Auditors with documentation to support their adherence to the protocols. This was followed by a visit to the force with HMIC Auditors conducting interviews with key staff. The visit to the force also incorporated the final stage of the inspection that was based upon reality checks. The reality checks focused on reviewing PNC arrest/summons and court result data against source 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 accepted 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)[1] 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 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 1896 (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 was increased to 75% on 1st July 2005, six months after the commencement of the code. (Courts have their own target of 3 days for delivery of the data to the police. Therefore, the police are currently measured against an overall target of 10 days).

1.4.4 Northamptonshire Police create arrest/summons records on PNC via an electronic transfer of information between the NSPIS custody application and the PNC. Records are transmitted directly to PNC when the custody record is closed by custody staff. The PNCB monitor the success of the electronic transmissions and also the quality of data being transmitted. At the time of the inspection, this process had only existed for approximately 4 weeks. The new process had had an initial impact on performance with the force suffering dips in performance in the run up to implementation and also in the first couple of months after the new process had gone live. Between February 2006 and November 2006, the force exceed the target of 90% in every month. Performance dropped between December 2006 and February 2007 when 81.4% of records were created within the target time of 1 day,

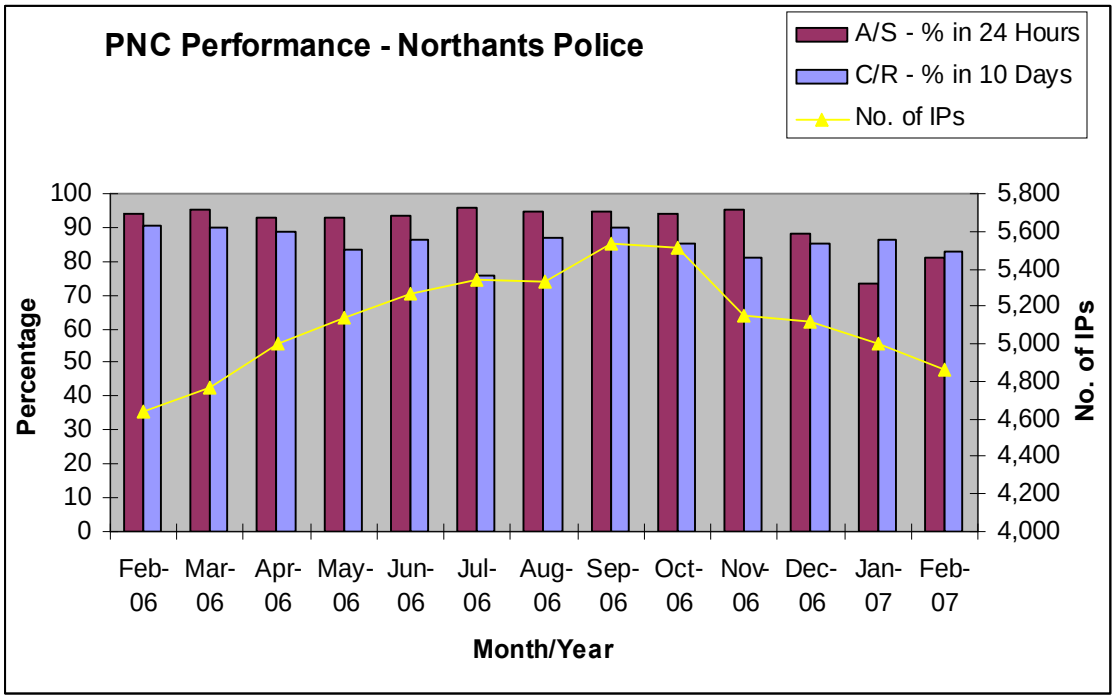
[1] As of 1st April 2007, Centrex and PITO now form part of the newly formed National Policing Improvement Agency (NPIA)

however, HMIC Auditors are confident that the force has adopted processes to minimise the impact of this performance shortfall.

1.4.5 Performance with regard to the input of court results has been consistently above the target of 75% over the last twelve months. In February 2006, the force entered 90.8% of results within 10 days. This had reduced slightly to 83% in February 2007, however, the new process for the creation of arrest/summons reports is a factor on this indicator. Nevertheless, the current performance still exceeds the target.

1.4.6 In terms of Impending Prosecutions (IPs), the overall number of outstanding IPs has shown a negligible increase from 4,642 in February 2006 to 4,866 in February 2007, an increase of 4.8%. HMIC Auditors are assured that the force has sufficient processes to ensure that the number of outstanding Impending Prosecutions is being managed.

1.4.7 A graph illustrating Northamptonshire Police's performance in the 12 months to February 2007 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. However, the key areas can be summarised as follows, identifying the areas of concern that have contributed to the grading:

- The force needs to increase activity in respect of Data Protection Auditing of data held on the PNC, an area of concern for HMIC.
- The force should also cease using non-accredited trainers for the delivery of training and the approval of new users for the system. Current practice is in breach of the Code of Connection for the PNC.
- Monitoring of Strategic Objectives for the PNC should ensure that all aspects of compliance are taken into account, reducing the risk of weaknesses that have been identified above.
- Bail Conditions and full records of court hearings are not updated on to the system.
- Effective processes are in place for the creation of Arrest/Summons reports.
- There is good liaison between the force and the courts, improving the provision of data relevant for update to the PNC.
- The submission of timely and quality data by officers is embedded into the culture of the force.

1.5.3 The findings of this report should be read in conjunction with the previous reports and recommendations relating to 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 seen in Appendix A of this report.

2. Detailed Findings and Recommendations

2.1 Leadership

2.1.1 The overall leadership for PNC issues rests with the Deputy Chief Constable (DCC) within Northamptonshire Police. HMIC Auditors found that the DCC demonstrates a good understanding of the issues regarding PNC and there is a clear interest to ensure that the force achieves the appropriate level of compliance.

2.1.2 Whilst the DCC has overall responsibility for PNC within the force, day to day responsibility is devolved through a structure of strategic groups within the organisation. The structure does not include a PNC Steering Group (PSG) in its own right because the group was merged with the Operational Intelligence Steering Group (OISG) during 2006.

2.1.3 The OISG is chaired by the Superintendent who carries out the role of Director of Intelligence. The group combines issues relating to intelligence and PNC and has a membership that is appropriate for combined terms of reference for the group. HMIC Auditors also reviewed the items that are discussed in the OISG and the frequency of the meetings. They were pleased to note that PNC issues remain evident within the minutes and that the group meets on a quarterly basis.

2.1.4 In addition to the membership of the group and the frequency of the meetings, HMIC Auditors also reviewed the Terms of Reference (ToR) for the group. The ToR have recently been rewritten following the re-structure of the strategic groups, to ensure that delivery of PNC issues provides benefits to the force both in terms of the use of PNC and compliance with relevant standards. The ToR states the membership of the group and also identifies the main functions of the group. Following the review of the group structure, HMIC Auditors are of the opinion that the ToR reflects the demands facing forces with regards to PNC and that merging the previous two groups has not had any negative impact on the strategic management of PNC within the force.

2.1.5 Despite the DCC not chairing the OISG, HMIC Auditors were satisfied that the appropriate lines of communication are in place if chief officer involvement becomes necessary. The Director of Intelligence meets with the DCC on a monthly basis, therefore, the mechanism exists to alert chief officers of contentious issues relating to the PNC. Overall, the structure of the groups was a strong area within the inspection, however, in view of some of the findings later in this report, HMIC Auditors are of the opinion that there is a need to ensure that all compliance issues are addressed within the group.

Recommendation 1

Her Majesty's Inspector of Constabulary recommends that the Operational Intelligence Steering Group (OISG) re-addresses all compliance matters from the PNC Code of Practice and ensures that progress towards delivery of these issues is monitored by the group.

2.1.6 HMIC Auditors also reviewed the level of accountability at all levels of the organisation in respect of the timely submission of data for update to PNC. This part of the inspection also examined the availability of management information to ensure that accountability can be measured and enforced.

2.1.7 Management Information in produced on a monthly basis by the PNC Bureau (PNCB) and is sent to senior managers and BCU Commanders in electronic format. Examples of the information that is produced was provided to HMIC Auditors and senior managers also provided anecdotal evidence that the format of the information ensured that any remedial action was easy to identify. Furthermore, the structure of management groups also ensures that exceptional issues are dealt with accordingly and that the relevant reporting lines exist.

2.1.8 In addition to the OISG which is focused on Intelligence and PNC, there is a Managing Performance Group (MPG) which covers all areas of performance. Both the OISG and MPG report to the Managing Knowledge Group (MKG) which is chaired by a chief officer and is the main strategic group within the organisation. Therefore, there is a robust mechanism to hold managers accountable for the performance of their respective BCUs. HMIC Auditors also discovered that in addition to managers being held to account, the performance regime is cascaded down to operational officers and that the need to submit timely data for update to PNC is embedded within their processes. During focus groups, anecdotal evidence was provided to support this finding.

2.1.9 Levels of accountability also extend to the PNCB. The PNCB produce the monthly statistics to provide an overview of the overall force performance, however, the unit also produces a monthly situation report to highlight its own performance. The situation reports also identify any action that is being carried out to ensure the force is achieving compliance. The production of these reports is considered as good practice by HMIC Auditors.

2.2 Policy and Strategy

2.2.1 With regard to policy and strategy, the inspection focused on a number of areas that warrant review. These can be described under the broad headings: PNC Policy & Strategy; Security and Data Protection. Each of these themes is discussed in further detail below.

2.2.2 PNC Policy & Strategy

2.2.2.1 Under this heading, HMIC Auditors reviewed whether the force has strategic direction or whether it is in a situation where it can only react to internal changes or external influences, for example, the publication of the code of practice. In addition, the number and types of policies were reviewed and also whether relevant staff are aware of the existence of certain policies.

2.2.2.2 Strategic direction for PNC is provided through the Terms of Reference of the OISG, complimented by the requirements of other strategic and performance groups (MPG & MKG). They were pleased to note that the force has developed comprehensive strategic plans for the PNC, including defined objectives of what the force wants to achieve. The documents are also supported by a strategic action plan in order that progress against the objectives can be monitored by the OISG.

2.2.2.3 However, whilst the action plan is a dynamic document that is updated to reflect changes at local or national level, HMIC Auditors identified an area for improvement with the document. Currently, actions arising from the results of data protection audits are not added to the plan. It is the opinion of HMIC Auditors that actions of this nature relating to PNC are monitored in a robust manner to provide assurance that risks to the data being processed on PNC by Northamptonshire Police are reduced.

Recommendation 2

Her Majesty's Inspector of Constabulary recommends that the Operational Intelligence Steering Group ensures that all potential sources of actions relating to the PNC are considered to ensure a proactive status is maintained.

2.2.2.4 With regards to force policy on PNC, HMIC Auditors were provided with copies of force policies and guidance in respect of the various functions on the PNC. All policies are comprehensive and provide sufficient information for staff who are required to use the PNC, or request information held on the system. All policies are individually referenced and are available via the force intranet. Furthermore, during interviews and focus groups, HMIC Auditors were pleased to learn that all staff are aware of the policies and their location if they were needed as a reference.

2.2.2.5 Within the PNCB, polices and guidance are complimented by individually documented process maps for every process conducted within the bureau. HMIC consider this to be good practice to ensure that consistent practices are maintained and that resilience is achieved.

2.2.3 Security

2.2.3.1 Under this section, HMIC Auditors reviewed the processes surrounding the management of user access to PNC and also the security policies that support the use of the system.

2.2.3.2 Administration of user access is currently carried out by the PNC trainers within the PNCB. The PNC trainers manage the creation or amendment of the user groups and assign users to groups depending on their role within the organisation. At the time of the inspection, there were approximately 80 separate groups providing tailored access for specific roles. Records of all trained staff are kept by the PNC trainers.

2.2.3.3 When people leave the force, their details are included in Force Orders which are published by the force on a weekly basis. Force Orders contain information on new policies and changes to existing policies but they also include information relating to staff who have left the force or staff who have changed roles within the force. The PNC Trainers review the staff changes on Force Orders and amend or delete PNC access if appropriate.

2.2.3.4 In addition to the review of force orders, the PNC trainers also monitor PNC use on a monthly basis. The #SU[2] transaction is carried out on the PNC to highlight any PNC User IDs that have not been used for over three months. Any User IDs that fall within this category have their access suspended. The PNC trainers contact the user to see if access is still required and if so, the user must attend refresher training before reactivation of the User ID. HMIC Auditors consider this to be good practice.

2.2.3.5 Whilst the process for managing user access is robust, HMIC Auditors of the opinion that the force will gain further assurance that all User IDs are current and relevant if the list of IDs is subject to an independent check. Whilst not questioning the integrity of the staff currently involved in the administration of User IDs, the process is currently being managed by staff who also have operational access to the PNC. This creates an additional risk to the organisation, therefore, the independent audit, or dip sample of User IDs will mitigate this risk.

Recommendation 3

Her Majesty's Inspector of Constabulary recommends that in order to gain assurance that all PNC User IDs are current and relevant, an independent audit or dip sample of the User IDS should be carried out on an annual basis.

2.2.3.6 Under this heading of the report, HMIC Auditors also examined the Information Security Policy (ISP) within the force. The policy was provided as part of the pre-read information requested by HMIC Auditors and it was reviewed to ensure it is both up to date and complete.

2.2.3.7 Information Security is the responsibility of the Information Security Manager within the Information Compliance Unit. A high level Force Information Security Policy (FISP) has been implemented which does not include specifics about individual systems. Policy documentation in respect of specific systems will take the form of the individual System Security Policies (SSPs), however, only those relating to systems classed as 'high impact' by the force are currently up to date. The reason for this is that in order to develop the SSP, systems owners have been identified to ensure that the risk assessment for the systems takes account of all relevant factors. With

[2] #SU - A Transaction on the PNC that lists all Users IDs that have not been used over a specified period of time.

regards to ‘low impact’ systems, the systems owners had not been identified at the time of the inspection.

2.2.4 Data Protection

2.2.4.1 Data Protection sits within the Information Compliance Unit which is a part of the Professional Standards Department (PSD). In terms of organisational positioning, this is considered to be good practice to ensure effective reporting lines exist.

2.2.4.2 However, despite the organisational positioning of the function, HMIC Auditors view this aspect of the inspection as an area of concern. At the time of the inspection, there was no risk based audit plan and only a limited amount of data protection auditing had been carried out over the previous 12 months. In addition, anecdotal evidence suggested that if a plan was produced using a risk based approach, there are insufficient resources available in order for the force to meet the demands of the plan. HMIC PNC Compliance Auditors are of the opinion that the level of auditing needs to be increased in order provide assurance that the force is complying with the Data Protection Act.

2.2.4.3 HMIC Auditors did learn that the force is planning the introduction of an Information Unit which will take over the responsibility for auditing. This will answer the concerns raised within the report, however, it will only be meet the requirements if sufficient and suitably skilled resources are made available to the unit.

2.2.4.4 In addition to the provision of a risk based audit plan, HMIC Auditors also reviewed the most recent audit reports that were available. In February 2006, an audit of the Wanted/Missing index of the PNC was subject of a force wide audit. The report was broken down by individual BCU, each receiving its own recommendations.

2.2.4.5 The reports provided BCU commanders with a snapshot of their own performance and highlighted the areas for improvement. However, there was no evidence that the recommendations made were being followed up to completion. If recommendations are not finalised, there is a risk that previous shortfalls in the processing of data could be replicated in the future, devaluing the results of the initial audit. HMIC Auditors are of the opinion that any recommendations made in respect of the PNC, should be published to the OISG to add to the strategic action plan. This will ensure that individual responsibility for delivery of the action is assigned, including timescales. The OISG can then monitor progress against the recommendations.

Recommendation 4

Her Majesty's Inspector of Constabulary recommends that in relation to Data Protection Auditing the force should:

▪ Ensure sufficient and suitably trained resources are available to carry out audits;

▪ Introduce risk based planning of audits in accordance with the ACPO Data Protection and Audit Manual:

▪ The OISG takes ownership of all recommendations made as a result of Data Protection audits of PNC. This will ensure that progress against all recommendations is monitored at an appropriate level.

2.2.4.6 As part of the inspection, a review of the process for transaction monitoring within the force was also conducted. Transaction monitoring is a process contained within the Data Protection Audit Manual (DPAM) that forces should use to determine the legitimacy of PNC transactions carried out by its operators. The DPAM states that a minimum of 3 per day should be conducted, although depending on the size of the force, the sample size should be representative of the overall number of transactions completed by the force.

2.2.4.7 In Northamptonshire Police, HMIC Auditors found that transaction monitoring is carried out by the Information Compliance Unit (ICU). The ICU selects transactions at random with an aim to check 25 transactions per week. Details of the transaction are sent direct to the operator via e-mail with a request for the operator to append the e-mail with the reason for the transaction and reply direct to ICU. There is no involvement of the operator's line manager.

2.2.4.8 Without the involvement of line managers in this process and insufficient resources within the ICU, HMIC Auditors discovered that if a reason for a transaction looked legitimate, the reason was automatically accepted and no further analysis was conducted. There is a risk to the organisation that operators could become wise to this weakness in the process. If there are staff who are susceptible to carrying out checks for reasons other than a policing purpose, opportunities are available for them to cover their activities.

2.2.4.9 HMIC Auditors are of the opinion that in order to reduce the risk of misuse of PNC by staff in Northamptonshire Police, the force should introduce measures to ensure that reasons for transactions are verified. This could include the endorsement of a line manager on the e-mail that is used by ICU for monitoring or that ICU dip samples the reasons that are provided. For example, if an incident number is provided as the reason for the transaction, the incident log should be examined by ICU or the line manager who provides the endorsement.

Recommendation 5

Her Majesty's Inspector of Constabulary recommends that the process for transaction monitoring should include either a check by line managers concerning the validity of the check, or a dip sample by data protection staff of the reasons provided.

2.2.4.10 Finally with regards to Data Protection and Information Security (DP/IS), HMIC Auditors considered the level of training that is available to staff in respect of these two aspects of the inspection. All inductions courses include a formal input on Data Protection using the Easy Eye computer based training product. The package continually assesses staff using assessments as they move through the training, assessments must be successful before further progress can be made. The product has the facility to provide training on Data Protection, Information Security, Freedom of Information and Government Protective Marking Scheme (GPMS), however, Northamptonshire Police are currently only utilising the Data Protection functionality. Information Security training is delivered in the form of handouts to new staff on the induction course.

2.2.4.11 This focus on new staff is good practice because staff are also required to sign a form indicating that they understand their responsibilities in relation to DP & IS. However, HMIC Auditors are of the opinion that Information Security should be considered as significant as Data Protection and therefore, a formalised input should also be delivered to new staff. The force should consider expanding the functionality of the existing software package to ensure delivery of this formal approach. Furthermore, the force should also investigate measures to ensure that existing staff are kept fully up to date with legislation. Anecdotal evidence was provided during focus groups that staff are unsure about what can or cannot be disclosed and that confusion surrounding DP/IS is prevalent throughout the force.

2.3 People

2.3.1 PNC Awareness

2.3.1.1 HMIC Auditors were unable to provide a true evaluation of their findings with regards to the level of awareness amongst staff. During the course of the inspection, the level of awareness had been perceived as high amongst all staff, however, it was discovered that all staff who had been selected to take part in the inspection had been provided with a briefing pack. HMIC Auditors do not question the intention of the packs, in that they were provided to place staff at ease regarding the format of the inspection, particularly those of junior ranks who had not been involved in the process before.

2.3.1.2 However, unintentionally, the packs provided staff with an overview of the PNC, highlighting aspects of the system that were relevant to the inspection process. Therefore, the levels of awareness that were perceived by HMIC Auditors cannot be considered as a true representation of the force as a whole because the levels of

awareness amongst staff who received the packs may now be higher than those who were not part of the inspection process.

2.3.1.3 Nevertheless, during interviews and focus groups when the format was on a more conversational basis, some staff clearly demonstrated a knowledge of the system and provided examples when the system had been put to good use, in particular in relation to the investigation of crime. Staff also commented on the provision of the PNC service within the force, for example, access to specialist knowledge when required and the availability of staff to provide routine checks, and in once focus group, a rough measure of the service was provided as being 9 out of 10.

2.3.1.4 In addition, the force has developed a marketing strategy as part of the overall l PNC Strategy. This strategy has its own separate action plan in order that the profile of the PNC is raised within the force. The marketing strategy outlines the target audience, the methodology and also includes evaluation to measure the effectiveness. This is good practice and is also considered a good template that can be used by any force who is considering the development of a marketing strategy.

2.3.1.5 Under this section of the report, HMIC Auditors also reviewed the process to ensure that new officers to the force receive relevant information about the PNC during their initial training. They were pleased to learn that the Initial Police Learning & Development Programme (IPLDP) contains an overview of the PNC at weeks 3 and 5. The overviews are sessions dedicated to the PNC and provide an input on the capabilities of the system and responsibilities of officers when using or submitting data to the system.

2.3.2 Training

2.3.2.1 PNC Training is provided by PNC training facility within PNC Bureau Crime Intelligence. At the time of the inspection, two members of staff were providing training on behalf of the force. HMIC Auditors found that the planning and delivery of training was being conducted in a way that meets the demands of the force, however, areas for improvement were identified and due to a fundamental failure on the part of the force, this aspect of the inspection is considered to be a concern.

2.3.2.2 PNC Trainers deliver enquiry training and update training separately. Enquiry level training, which enables users to interrogate records only, is being delivered through the use of Supported Learning Modules (SLMs). SLMs provide a structured learning process where students learn at their own pace in a training room where support is available from a trainer. The use of SLMs enables students at different stages of progression to be trained simultaneously by one trainer, thereby making best us of the trainer's time and increasing access to the training facility to all students. Positive feedback was provided to HMIC Auditors from staff who have started or completed training using an SLM.

2.3.2.3 Update training, which allows operators to amend or create records on the system remains confined to a classroom environment due to the complexities of some of the updates. The content and duration of training is to the required standard as set out by Centrex (now part of the newly formed National Policing Improvement Agency – NPIA). Due to updates being carried out at a limited number of sites, the force is

able to manage the planning and delivery of the training. Anecdotal evidence from staff in posts that require update training reflects this opinion.

2.3.2.4 However, the fundamental failure referred to earlier that has caused this aspect of the inspection to be cause for concern is that the force is using a non-accredited trainer for the delivery of PNC training, for the endorsement of students completing SLMs. The standard laid down by Centrex is that in order to ensure a consistent approach to the delivery of training, all training must be delivered by accredited PNC trainers. it was noted that;

"*It is a requirement of the code under which forces are connected to PNC that all persons having access to PNC must have received the correct training. It has also been agreed, by the PNC Director, NPT and user groups, that training will only be delivered by trainers who have successfully attended the nationally accredited PNC Trainers Course."*[3]

2.3.2.5 Further information was provided to HMIC Auditors that all training and work carried out by the non-accredited trainer is checked by an accredited trainer. However, this was not part of any formal development or training programme that the non-accredited trainer is following. There were also no plans to have the member of staff accredited by Centrex. That was in part due to the current member of staff being temporarily employed to cover a long term absence within PNC Training. HMIC Auditors are of the opinion that the force must decide on the long term plans for PNC training, particularly to provide resilience if long term absences occur in the future. In the interim period, only PNC trainees that have been trained and approved by an accredited PNC trainer should be given access to the system.

Recommendation 6

Her Majesty's Inspector of Constabulary recommends that the force immediately stops the use of a non-accredited PNC trainer for the delivery or approval of PNC Training and considers options for providing resilience on a long term basis in respect of PNC training.

2.3.2.6 With regards to the areas for improvement that were identified in the planning and delivery of training, HMIC Auditors found that there is no corporate policy on which members of staff, or which roles should be identified for receiving PNC training. Approval for PNC Training is provided at BCU level, however, with no corporate policy, there is a risk of staff in certain roles on one BCU being offered training places, whilst staff in similar roles on a different BCU being refused. This does not affect any staff who have training approved because once it has been approved, the PNC training is delivered, however, there is a risk that inconsistencies exist in the criteria being used in each BCU when decisions are being made. The only pre-requisite for staff attending PNC course is that they should have a general knowledge of I.T. Furthermore, when the #SU transaction is carried out to identify staff who have not used the system (see para 2.2.3.4), no analysis of the roles of staff who are not using the system is carried out. If such analysis was done, the

[3] 'On The Record – Thematic Inspection Report on Police Crime Recording, the Police National Computer and Phoenix Intelligence System Data Quality' P.115, Paragraph 7.5.2

findings could be used to formulate future PNC training strategy, enabling additional efficiency benefits for the training team.

Recommendation 7

Her Majesty's Inspector of Constabulary recommends that in order to provide a more efficient approach to the delivery of PNC training, Northamptonshire Police develop role profiles to define the levels and types of training required for each role.

2.3.2.7 A further area for improvement in respect of PNC Training is in relation to evaluation. At the time of the inspection, evaluation was only carried out in the form of feedback forms (commonly known as 'Happy Sheets') that are distributed to students at the end of the course. There is no further evaluation once the student has returned to the workplace, to determine whether the course met the objectives that the student expected.

2.3.2.8 Formal evaluation of this nature can be a major administrative exercise, therefore, HMIC Auditors are of the opinion that in order to gain some benefit from the process, the force should consider a dip sample of students who complete PNC training. As a result of anecdotal evidence, HMIC Auditors discovered that this level of evaluation does take place for training carried out by the force training school, therefore, the scheme should be expanded to include all training done within the force.

Recommendation 8

Her Majesty's Inspector of Constabulary recommends that the force considers the expansion of training evaluation to include PNC training courses carried out by PNC CI Trainers.

2.3.2.9 On a positive note in respect of PNC training, HMIC Auditors consider the use of 'in-service' training as good practice. The force uses an opportunity afforded by the organisational positioning of PNC training, of keeping all staff in the PNCB up to date with developments and changes to PNC. If changes occur that impact on the role of staff within the PNCB, 'in-service' training is planned. 'In-Service' training is ad-hoc training that is delivered in short sessions that concentrate on particular issues. The result is that staff receive formal, structured training but without the need for long periods of abstraction from their regular duties.

2.3.2.10 In addition, further good practice was evident in the use of Positive Action Status (PAS). PAS is used when staff are in need of development, either as a new starter within the unit, or if a performance issue has been identified. PAS provides line managers with a structured process to track the development of staff, including the production of action plans and programmes for training. PAS is time bound with staff being required to meet certain performance measures in order to be removed from PAS.

2.4 Partnerships and Resources

2.4.1 The development of relationships between the Force and other agencies is important to ensure that data exchanged between agencies is done so in a timely manner. Northamptonshire Police have taken the initiative in this area and introduced a tripartite meeting between themselves, the magistrates' courts and the crown courts. Meetings are held on a quarterly basis and provide an opportunity for each agency to highlight any issues in respect of the provision of court results that require update on to the PNC.

2.4.2 Staff reported that the quarterly meetings with the courts have resulted in benefits for the police in that the force now receives details of court disposals in a timely manner. Furthermore, the meetings have enabled the force to develop relationships with key members of staff within each court in order that queries can be addressed quickly. Other benefits have included exchange visits by staff from each organisation to gain an appreciation of how their counterparts work. This has resulted in queries being dealt with more efficiently by sending information to the correct staff at the first point of contact.

2.4.3 HMIC Auditors also reviewed the existence of any data sharing protocols that exist between the force and their partner agencies. These agreements are made under the auspices of the Data Protection Act and whilst HMIC Auditors were pleased to note that the force had a number of agreements, held centrally for ease of access for PNC operators, anecdotal evidence was provided that there had been little or no involvement from the Data Protection team. It is the opinion of HMIC Auditors that the Information Compliance Unit should take an active role in the development of these agreements to ensure that all agreements comply with the legislation. Once agreements have been made, they should pass to the PNCB but should remain the ownership of the ICU.

2.4.4 Under this section of the report, HMIC Auditors also reviewed any Service Level Agreements (SLAs) that the force has with non-police prosecuting agencies (NPPAs). At the time of the inspection, the force did not have any SLAs between itself and NPPAs, however, HMIC Auditors were informed that a number of SLAs are under development. HMIC Auditors would encourage the force to complete this process to ensure the timely and accurate of information originating from their partner agencies.

Recommendation 9

Her Majesty's Inspector of Constabulary recommends that the Force in conjunction with Non-Police Prosecuting Agencies, develop service level agreements to ensure timely submission of data for update to PNC.

2.5 Processes

2.5.1 In terms of processes, HMIC Auditors reviewed a number of issues within Northamptonshire Police that are worthy of note in this report. These relate to the creation of Arrest/Summons reports, court results, bail conditions, data quality, warning signals, ad-hoc intelligence updates and ViSOR.

2.5.2 Creation of Arrest/Summons Reports

2.5.2.1 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

2.5.2.2 At the time of the inspection, Northamptonshire Police had recently implemented the PNC interface within the NSPIS Custody application. Prior to this, creation of arrest/summons (A/S) reports was as a skeleton record which was created on the PNC by the PNCB following receipt of a faxed copy of the front page of the source input document from the arresting officer. In addition, PNCB could also retrieve information from the legacy custody system in order to create the initial record. Full update of the record was completed following the subsequent submission of a hard copy source input document by the officer. The process of faxing the front page of the source input document still exists for non-custody cases, e.g. Penalty Notices for Disorder (PNDs). HMIC Auditors discovered during focus groups that the need for timely submission of data was embedded into the culture of the force, ensuring that all officers were aware of their requirements. As a result of the implementation of the interface, the process for the creation of A/S reports changed significantly and the force suffered from an initial negative impact on their statistical performance.

2.5.2.3 The introduction of the new process now results in full records transferring directly from the custody application to the PNC once the custody record has been closed by custody staff. The direct link between the custody application and PNC is reliant on accurate data being recorded on the custody record in order to reduce the risk of transmissions over the interface failing. HMIC Auditors were pleased to note that the force has implemented procedures to counter this risk and that initial problems of failed transmissions was now being managed.

2.5.2.4 Staff within the PNCB monitor the transmission log on the NSPIS application, a facility that reports the success or failure of all transmissions, on a daily basis to ensure that any failures are dealt with expeditiously. Furthermore, when failures have occurred, the reason (or reasons) for the failure are recorded. The information is then passed to the project team responsible for the implementation of the interface to ensure that lessons learned or changes in procedure can be articulated to the custody suites. The management of the implementation has resulted in the force minimising the impact of the change in process, which is evidenced by recent performance which showed an initial drop, followed by a gradual improvement.

2.5.2.5 Whilst the force is managing the transfer of records from the custody system, there was also a backlog of hard copy source input documents that had not been input to PNC prior to the interface going live. The recent change in process will not add to the backlog and the force is taking action to reduce the volume on a monthly basis. Nevertheless, the force is encouraged to clear the backlog as soon as possible to ensure that accurate and complete records are recorded on the PNC.

2.5.3 Court Results

2.5.3.1 Court results are managed by a specific section within the PNCB. Magistrates results are received direct into the PNCB onto a printer that is linked to the Equis[4] system. Information is printed once the courts' staff have validated the data from the days court hearings. Crown Court results are received via the Xhibit portal and are matched to indictments that are faxed through from the crown courts.

2.5.3.2 Staff within the PNCB update the PNC direct with all disposals from the court register. All disposals from crown courts are also updated direct onto the PNC. This process works well for the force as they consistently achieve the target for entering disposals. However, the achievement of this target is at the cost of omitting the entry of other data from the court register onto the PNC.

2.5.3.3 Details of remands and unconditional bail are not recorded on PNC by the force. This results in inaccurate data being shown against A/S reports on the system and can lead to inefficiencies for all forces if they require up to date information about a case. The force is therefore encouraged to investigate opportunities for increased capacity that the interface can bring, to ensure that full and accurate records are updated on the PNC.

Recommendation 10

Her Majesty's Inspector of Constabulary recommends that the force investigates opportunities to ensure that all relevant data from court registers is updated on the PNC. Efficiency gains from the implementation of the NSPIS interface are an example of such opportunities.

2.5.4 Data Quality

2.5.4.1 Under this heading, consideration was given to the process for the quality assurance (QA) of updates to Arrest/Summons reports and court results. In addition to the examination of the process, HMIC Auditors also reviewed a number of records on the PNC against source documents to check the level of accuracy of the records that had been updated, referred to as reality checks.

2.5.4.2 Updates within the PNCB are checked on peer basis with staff checking each others work, depending on various factors. These factors include the experience of an operator, for example, new staff have 100% of their work quality assured, whether a member of staff has Positive Action Status (PAS) or whether there have

[4] Equis – computer system used by HMCS in the Northamptonshire area

been previous performance issues with a member of staff. Results of the QA are passed to team leaders within the PNCB who collate the results on a spreadsheet. Individual results are then provided in a report to each member of staff at the end of every month, highlighting the volume of errors that have been made and providing copies of the errors.

2.5.4.3 The QA reports on each member of staff are then used as part of the Personal Development Review (PDR) process. HMIC Auditors consider this to be good practice for the development of staff.

2.5.4.4 The QA process within the PNCB was evidenced by the negligible number of errors that were found during reality checks carried out by HMIC Auditors. From a sample of 32 source input documents for the creation of A/S reports that were provided to the auditors, none of the records (0%) contained an error. With regards to court results, a sample of 30 disposals was reviewed, with 20% of the records containing errors. These errors were classified as minor errors, ranging from spelling and typographical errors, to a failure to record the number of offences 'Taken into Consideration' on one case. The errors on the disposals were deemed to be minor because the criminal history would not have an impact on the future handling of a defendant, nor would there be any adverse impact on the force as a result of disclosure.

2.5.4.5 However, there was concern in some cases regarding the information contained on records where the disposals had been updated for serious offences. In 3 out of 8 crown court cases that were checked, offences were so serious (supply drugs and firearms offences) that they justified warning signals on the records. In the 3 cases checked, no warning signals had been updated on the records. (See Para 2.5.5)

2.5.5 Warning Signals

2.5.5.1 Warning signals are a key element to a persons PNC record in that they provide a reference that can be used to either protect the safety of an officer who deals with a nominal in the future, or can protect the nominal if ever they are taken into the custody. Examples of warning signals range from informing officers whether a person may be violent, carry weapons, use drugs or even whether they are known to have suicidal tendencies.

2.5.5.2 In Northamptonshire, the process for requesting a warning signal is by one of two methods. The first and most common method would be following an arrest when a an entry is made on the custody system. An officer will update the online source document to request a warning signal. Alternatively, if no offence has occurred but the officer feels there is a need to have information recorded, an e-mail can be sent to the PNCB requesting that an update is made to a nominal record.

2.5.5.3 Whilst the process appeared robust and all staff were aware of how warning signals were managed, HMIC Auditors found a number of serious cases which justified the presence of a warning signal but none were recorded and remain to be assured that all relevant warning signals are being recorded. In view of this, it is recommended that the force reviews the current process for the recording of

warning signals. The review should focus on ensuring that when updates are made to the record, operators consider all data items that may be relevant to a case. For example, checking for warning signals when they apply court results.

Recommendation 11

Her Majesty's Inspector of Constabulary recommends that the force reviews the current process for the input of Warning Signals. The review should ensure that all opportunities for identifying the requirement for a warning signal are considered, including the initial submission by an officer, update of an arrest by a PNC operator, update of results and the quality assurance process.

2.5.6 Ad-Hoc Intelligence Updates

2.5.6.1 Ad-hoc intelligence updates are updates that are made to the PNC where the source of the information is other than an arrest or summons where a source document would be used.

2.5.6.2 In Northamptonshire Police, there is no formal process for recording ad-hoc intelligence update on the PNC. The only ad-hoc updates that are made result from applications that originate from the Criminal Records Bureau (CRB). Staff on the disclosure section of the PNCB receive the applications and if the address on the applications differs to that already held on the PNC, the PNC is updated to reflect the most up to date information.

2.5.6.3 During interviews and focus groups, HMIC Auditors asked staff whether they had submitted any data for update to PNC, from a source other than an arrest. In all cases, staff reported that they did not know that a process existed to facilitate this kind of update. The force should review the existing arrangements and communicate the process to officers to ensure that relevant data is updated on the PNC. The review should ensure that only intelligence that has been evaluated should be considered for update. This approach will ensure that the credibility of information recorded on the PNC is maintained. Any change in process should also be supported by the introduction of a formal policy.

Recommendation 12

Her Majesty's Inspector of Constabulary recommends that the force reviews the current process for supplying ad hoc updates to the PNC. The review should focus on the reiteration of force policy and the evaluation of intelligence prior to update to the system.

2.5.7 Violent & Sexual Offenders Register (ViSOR)

2.5.7.1 ViSOR is a system to enable Public Protection Staff to manage and monitor known offenders that are living in the force area. The system draws information from the PNC when records are created and there are in-built audit transactions to highlight any activity on a ViSOR record.

2.5.7.2 One key aspect of the system is that the existence of a ViSOR record for a person who is known on the PNC will create a ViSOR warning marker on the PNC. This is used to alert officers that a nominal is a ViSOR subject. It is therefore important that the records on ViSOR and PNC both contain correct and up to date information. HMIC Auditors reviewed the process for ensuring that records on both system remain synchronised within Northamptonshire.

2.5.7.3 ViSOR records are centrally managed by the Dangerous Persons Management Unit (DPMU) at the Force Intelligence Bureau based at the site of the force headquarters. Any updates to a ViSOR nominal become known to the DPMU who update 'Home Visit Records' on the system. The PNCB can identify these updates from the ViSOR and update PNC directly. For updates the other way, from PNC to ViSOR, the inbuilt audit transactions of ViSOR enable the DPMU to be made aware that records have been updated.

2.5.7.4 HMIC Auditors also queried the level of knowledge amongst officers about ViSOR and although there was generally a good knowledge in those that were interviewed, the distribution of briefing packs, as referred to in paragraph 2.3.1.2, should be taken into account.

2.5.8 Bail Conditions

2.5.8.1 Bail conditions should be placed on the PNC to alert other forces that conditions may have been imposed elsewhere in the country. Currently, Northamptonshire Police do not update the PNC with bail conditions that have been issued by a magistrate. The only bail conditions that are recorded are police bail, when a person is baled to return to the custody suite, or those issued at crown court.

2.5.8.2 Magistrates court bail is notified to the force, either to local intelligence staff or to the Force Communication Centre (FCC). If local intelligence staff receive the information, the Force Intelligence System (FIS) is updated. However, if FCC receive the notification, a manual record is kept and retained in the FCC. This results in significant inefficiencies for FCC staff if they are required to check for the existence of bail conditions. They must check three systems, PNC, FIS and the manual record. Furthermore, if the information is only held locally and not on PNC, other forces would not be alerted to the fact that bail conditions exist. HMIC Auditors are therefore of the opinion that the force considers the current inefficient process with a view to recording all bail conditions on the PNC.

Recommendation 13

Her Majesty's Inspector of Constabulary recommends that in order to provide an efficient process for FCC staff and make bail conditions available on a national basis, the force commence updates of bail conditions to the PNC.

2.6 Results

2.6.1 In the 12 months to February 2007, Northamptonshire Police had maintained a consistent performance against the target for the creation of A/S reports. Up to December 2006, the force consistently achieved performance in excess of the target of 90%. Performance ranged from 92.9% to 96% between February and November. In December, the force suffered a drop in performance as the transition was made to the new interface. Performance in December dropped to 87.9%, then further to 73.6% in January when the interface went live. However, despite initial teething problems, the signs of recovery are already in place with the force increasing slightly to 81.4% in February 2007. This latest performance is just below the national average of 85.2%. HMIC Auditors are confident that with the monitoring processes being employed, the force should continue to improve on the recent performance slump.

2.6.2 Despite the change over to the interface, performance with regard to the input of court results has remained consistent throughout. In the twelve months to February 2007, the force exceeded the target in every month with performance ranging from 75.7% to 90.8% against a target of 75% within 10 days. The most recent performance in February 2007 showed that 83% of disposals were applied to the PNC within 10 days of the disposal date. This performance is also in excess of the national average for England and Wales of 71.1%.

2.6.3 In terms of Impending Prosecutions (IPs), the overall number of outstanding IPs has increased slightly 4,642 in February 2006 to from 4,866 in February 2007, an increase of just 224. HMIC Auditors learned that a continual process is in place to ensure that old cases are reviewed on a regular basis to provide assurance to the Force that all cases are legitimately outstanding. Every three months, data is received from the Hendon Data Centre containing information on old IPs. The information is uploaded to a spreadsheet which is used by a specific section within the PNCB to monitor the legitimacy of each case. HMIC Auditors are assured that this process ensures that the force is able to manage its old impending cases.

Appendix A

A Summary of Good Practice within Northamptonshire Police

- Update staff in the PNCB are provided with individual monthly reports outlining their performance. The reports are used as part of the PDR process.
- Documented process maps exist for every process carried out in the PNCB, providing clear guidance to staff.
- Staff must complete refresher training in order to regain access to the PNC if they have not used the system for over 3 months.
- A marketing strategy has been developed with a separate action plan to the main PNC Strategy. This enables the force to monitor progress and evaluate the effectiveness of the actions.
- In-Service training is provided to PNCB staff to keep them up to date with current procedures.
- The use of Positive Action Status (PAS) to assist in the development of staff.

Summary of Recommendations for Northamptonshire Police

Recommendation 1

Her Majesty's Inspector of Constabulary recommends that the Operational Intelligence Steering Group (OISG) re-addresses all compliance matters from the PNC Code of Practice and ensures that progress towards delivery of these issues is monitored by the group.

(Paragraph 2.1.5)

Recommendation 2

Her Majesty's Inspector of Constabulary recommends that the Operational Intelligence Steering Group ensures that all potential sources of actions relating to the PNC are considered to ensure a proactive status is maintained.

(Paragraph 2.2.2.3)

Recommendation 3

Her Majesty's Inspector of Constabulary recommends that in order to gain assurance that all PNC User IDs are current and relevant, an independent audit or dip sample of the User IDS should be carried out on an annual basis.

(Paragraph 2.2.3.5)

Recommendation 4

Her Majesty's Inspector of Constabulary recommends that in relation to Data Protection Auditing, the force should;

- ensure sufficient and suitably trained resources are available to carry out audits;
- introduce risk based planning of audits in accordance with the ACPO Data Protection and Audit Manual;
- the OISG takes ownership of all recommendations made as a result of data protection audits of PNC. This will ensure that progress against all recommendations is monitored at an appropriate level.

(Paragraph 2.2.4.5)

Recommendation 5

Her Majesty's Inspector of Constabulary recommends that the process for transaction monitoring should include either a check by line managers concerning the validity of the check, or a dip sample by data protection staff of the reasons provided.

(Paragraph 2.2.4.9)

Recommendation 6

Her Majesty's Inspector of Constabulary recommends that the force immediately stops the use of a non-accredited PNC trainer for the delivery or approval of PNC Training and considers options for providing resilience on a long term basis in respect of PNC training.

(Paragraph 2.3.2.4)

Recommendation 7

Her Majesty's Inspector of Constabulary recommends that in order provide a more efficient approach to the delivery of PNC training, Northamptonshire Police develop role profiles to define the levels and types of training required for each role..

(Paragraph 2.3.2.5)

Recommendation 8

Her Majesty's Inspector of Constabulary recommends that the force considers the expansion of training evaluation to include PNC training courses carried out by PNC CI Trainers..

(Paragraph 2.3.2.7)

Recommendation 9

Her Majesty's Inspector of Constabulary recommends that the Force in conjunction with Non-Police Prosecuting Agencies, develop service level agreements to ensure timely submission of data for update to PNC.

(Paragraph 2.4.4)

Recommendation 10

Her Majesty's Inspector of Constabulary recommends that the force investigates opportunities to ensure that all relevant data from court registers is updated on the PNC. Efficiency gains from the implementation of the NSPIS interface are an example of such opportunities.

(Paragraph 2.5.3.3)

Recommendation 11

Her Majesty's Inspector of Constabulary recommends that the force reviews the current process for the input of Warning Signals. The review should ensure that all opportunities for identifying the requirement for a warning signal are considered, including the initial submission by an officer, update of an arrest by a PNC operator, update of results and the quality assurance process

(Paragraph 2.5.5.3)

Recommendation 12

Her Majesty's Inspector of Constabulary recommends that the force reviews the current process for supplying ad hoc updates to the PNC. The review should focus on the reiteration of force policy and the evaluation of intelligence prior to update to the system..

(Paragraph 2.5.6.3)

Recommendation 13

Her Majesty's Inspector of Constabulary recommends that in order to provide an efficient process for FCC staff and make bail conditions available on a national basis, the force commence updates of bail conditions to the PNC.

(Paragraph 2.5.8.2)

Appendix B

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

Recommendation 9 (Chapter 5 page 86)

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

Recommendation 10 (Chapter 6 page 104)

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

Recommendation 11 (Chapter 7 page 111)

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

Recommendation 12 (Chapter 7 page 112)

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

Recommendation 13 (Chapter 7 page 118)

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

Recommendation 14 (Chapter 8 page 145)

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

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

Recommendation 15 (Chapter 8 page 146)

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

Recommendation 16 (Chapter 8 page 148)

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

Recommendation 17 (Chapter 8 page 150)

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

Recommendation 18 (Chapter 9 page 164)

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

Recommendation 19 (Chapter 9 page 164)

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

Recommendation 20 (Chapter 9 page 165)

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

Appendix C

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 D

Police National Computer Data Quality and Timeliness – 1st Report

Recommendation One (Paragraph 5.2)

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

Recommendation Two (Paragraph 5.11)

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

Recommendation Three (Paragraph 5.19)

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

Recommendation Four (Paragraph 5.29)

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

Recommendation Five (Paragraph 5.31)

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

Recommendation Six (Paragraph 5.34)

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

Recommendation Seven (Paragraph 6.10)

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

Recommendation Eight (Paragraph 6.12)

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

Recommendation Nine (Paragraph 6.14)

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

Recommendation Ten (Paragraph 6.16)

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

Appendix E

Police National Computer Data Quality and Timeliness – 2nd Report

Recommendation 1

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

Recommendation 2

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

Recommendation 3

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

Recommendation 4

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

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

Recommendation 5

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