KENT POLICE

8 – 12 AUGUST 2005

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 Kent Police between 8th and 12th August 2005.

1.1.2 Kent 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 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 two of the nine Basic Command Units (BCUs). These views have been supported by reality checks conducted by HMIC PNC Compliance Auditors.

1.2 Background

1.2.1 Kent Police covers an area of approximately 1,443 square miles in the south east of England. Local policing is managed at nine BCUs (known locally as Areas) at North Kent, West Kent, Maidstone, Medway, The Weald, Swale, Canterbury, Thanet and South East Kent. The resident population of the county is approximately 1.6 million, however, policing challenges are increased with over 33 million cross-channel passengers passing through the county on an annual basis en route to the channel tunnel or one of the major ferry ports, providing access to Belgium and/or France. The county is also home to Bluewater, the largest retail park in Europe, which also attracts 27 million visitors a year. In addition, the county is home to two migrant reception centres at Ashford and Cranbrook, contributing the significant population of asylum seekers within the county. There are also two nuclear power stations sited within the county, on the Dungeness peninsular.

1.2.2 The Force is headed by the Force Command Team, led by the Chief Constable, supported by the Deputy Chief Constable (DCC), three Assistant Chief Constables (ACCs), with individual responsibilities for Central Operations, Area Operations and Personnel & Training. There is also a Director of Finance & Administration. The Force strength comprises approximately 3,600 full-time equivalent police officers, 2,400 police staff, 330 Special Constables and 58 Police Community Support Officers (PCSO).

1.2.3 The PNC function falls within the portfolio of the ACC Central Operations who has overall responsibility for the function. However, day to day management of the function is devolved to a Superintendent in charge of the Intelligence & Information and the manager of the Force Information Bureau (FIB). The FIB manager, who also carries out the role of PNC Liaison Officer, is responsible for the staff who update Arrest/Summons information, court results, MO keywording and vetting & disclosure.

1.2.4 The FIB, based at the force headquarters, comprising approximately 70 staff is divided into four sections. The Operational section maintains a 24 hour/7 day presence within the unit and are responsible for the creation of Arrest/Summons reports and making operational updates to PNC, for example, the creation of Wanted/Missing circulations on the PNC. The Resulting and Quality Control sections work between 07:00 and 24:00 Monday to Friday and the Disclosure section are in attendance between 08:00 and 24:00 hours Monday to Friday.

1.2.5 The FIB is responsible for all updating of the names application throughout the force, including arrest/summons, court results, bail conditions, MO keywords, wanted/missing, disqualified driver updates and quality control. An arrest/summons report is created on the PNC following a telephone call from the officer in the case when a person is arrested. The information provided on the telephone is sufficient to create a skeleton record with the officer in the case providing full information by submitting a hard copy source document, known as the 1837a, via the internal mail system. The operational section of FIB takes the initial calls and is also responsible for the full completion of the record upon receipt of the 1837a.

1.2.6 Court results are sent to FIB via an interface between the courts system (Equis) and the forces own integrated system (Genesis). Results are sent individually from the courts when they have been validated by courts staff and notification to the force is in the form of an e-mail providing details of the case. Staff from the resulting section update court disposals directly to PNC. Crown court results are received manually via the DX postal system to the Crown Court Liaison staff, based at the force headquarters, on a daily basis, where they are subsequently collected by a member of staff from FIB.

1.2.7 VODS (Vehicle On-line Descriptive Searches) and QUEST (Queries Using Enhanced Search Techniques) searches are also provided by FIB. FIB operate as a central point of contact for the whole force and are the only operators, other than very few exceptions, who can conduct these searches. Staff on the operational section of FIB carry out the enquiries, ensuring that a 24hour/7 day facility is provided.

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 PNC Compliance Auditors with documentation to support their adherence to the protocols. This was followed by a visit to the force with HMIC PNC Compliance 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 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) 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).

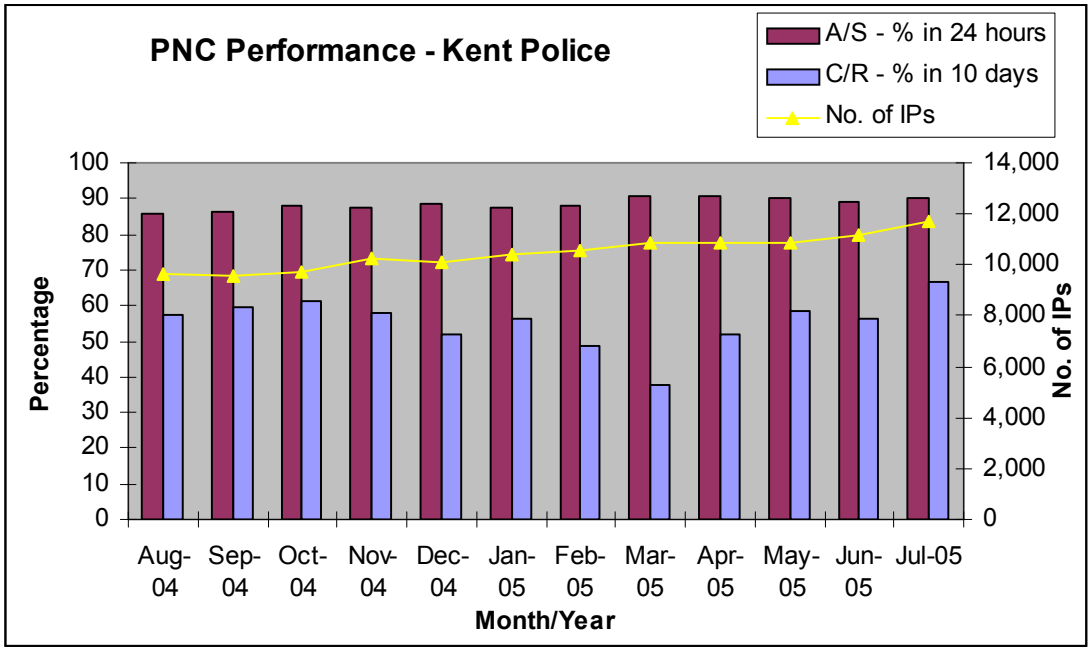
1.4.4 Kent Police create arrest/summons records on PNC via a telephone call from the arresting officer to the FIB. Initial details are recorded to create a skeleton record on PNC to provide an Arrest/Summons reference number to be used by the officer on fingerprints and DNA samples. Completion of the full record is carried out following the submission of a hard copy descriptive form (1837a) by the officer to the FIB after the skeleton record has been created. In the 12 months to July 2005, the force has maintained performance at the target level of 90% or just below. In August 2004 the force achieved 86% within 24 hours rising to a high of 90.7% in March 2005. The most recent performance data, July 2005 shows that 90.3% of records were created within the target time of 24 hours. In terms of the number of days to enter the quickest 90% of records, the force has gradually reduced this figure from three days in August 2004 to 1 day in July 2005, achieving the target on a regular basis. The

force is performing higher than the England and Wales national averages for this aspect of PNC Performance.

1.4.5 Performance with regard to the input of court results has shown an upward trend other than a slight dip for two months early in 2005. When the Code of Practice for PNC was introduced in January 2005, the force met the target of 50% in January 2005. However, despite a dip to 37.5% in March 2005, performance has since improved to 66.9% in July 2005. Whilst this remains outside of the revised target of 75%, the force has taken steps to identify the reasons for this and is already taking remedial action to improve the overall performance. With regard to the number of days taken to meet the respective targets within the Code of Practice, 50% between January and June and 75% from July 1st, the force has steadily reduced the number of days. In June 2005, it was taking 8 days to meet the target of 50%. In July 2005, it took the force 14 days to meet the new target of 75%, however, HMIC PNC Compliance Auditors are satisfied that the remedial action mentioned above will address this drop in performance.

1.4.6 In terms of Impending Prosecutions (IPs), the overall number of outstanding IPs has increased from 9,545 to 11,734 between August 2004 and July 2005, an increase of approximately 23%. However, there is a direct correlation between the increase in the number of IPs and the implementation of the Criminal Justice Act. HMIC PNC Compliance 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

1.4.7 A graph illustrating Kent Police's performance in the 12 months to July 2005 is shown below.



1.5 Conclusions

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

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

1.5.2 This assessment is based on the detailed findings of the report. However, the key areas can be summarised as follows:

- The force needs to ensure that activity surrounding PNC is at a corporate level and not being carried out in isolation within different BCUs.
- The level of accountability on individual officers needs to be increased concerning the timeliness and quality of information being submitted for update to PNC.
- Clear Strategic Objectives need to be defined and documented to ensure that progress can be monitored.
- The process of Data Protection auditing in need of review to ensure that the force is gaining maximum assurance from the unit.
- Levels of awareness amongst staff are good with the PNC.
- There are a number of weakness in detailed processes that are affecting the forces ability to experience sustained improvement

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 ACC Central Operations within Kent Police. HMIC PNC Compliance Auditors found that the current ACC has a good level of knowledge and understanding of issues relating to PNC, with a clear interest to ensure that the force improves to a position in which compliance is being achieved.

2.1.2 The force has recently re-structured the strategic management of PNC by removing the PNC Steering Group as an entity in its own right and replacing it with a new structure under the auspices of the Bichard Information Management Board (BIMB). The BIMB is chaired by the ACC Central Operations and has four sub-groups that report directly to the board. One of the groups is the PNC Sub-Group (PsG) which is chaired by the Chief Superintendent who is head of Criminal Justice.

2.1.3 The membership of the PsG consists of all relevant personnel throughout the force, however, HMIC PNC Compliance Auditors felt that an increased presence from BCU staff would be beneficial. BCU staff play an significant role in achieving compliance, therefore, representation on the sub-group is important to ensure they are aware of their responsibilities and also to take opportunities to disseminate good practice. .In addition, the sub-group has recently been meeting approximately every 6 weeks. This frequency is currently out of step with the BIMB which is planned to meet on a quarterly basis and it also poses the risk of apathy amongst the group members if there is no update on actions because insufficient time has elapsed between meetings. The force has identified this as an issue and is currently reviewing the frequency and timing of the meetings in order to ensure that they coincide with BIMB meetings.

2.1.4 In addition to the membership of the group and the frequency of the meetings, HMIC PNC Compliance 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, for example, the Code of Practice and Bichard recommendations. The ToR is based around what the force has named ‘six key business strands’ encompassing all relevant issues for the delivery of PNC compliance. The six strands are; Service Delivery, Data Quality, Data Creation Working Practices, Performance Monitoring, Change Management and Training & Development. HMIC Auditors are satisfied that the ToR reflects the demands facing forces with regards to PNC.

2.1.5 HMIC PNC Compliance Auditors also reviewed the level of accountability placed upon officers concerning the submission of data for update to PNC and the use of management information to support this process. HMIC PNC Compliance Auditors found that although management information is provided by FIB to BCU commanders, the depth of the information is not sufficient for the BCU command team to deal with under performance at an individual level. The current level of management information is providing BCU commanders with more questions to ask, rather than providing the answers, or reasons, why performance is not being achieved. For example, BCU commanders receive information on the timeliness of the creation of arrest/summons reports for each area, however, they are not provided with information that may identify whether any shortfall is from a particular relief, or an individual officer. The BCU commander currently has to initiate further analysis in order to identify areas for improvement.

2.1.6 In one BCU, a recent initiative has been started in the Criminal Justice Unit (CJU) to overcome this shortfall in information. Staff in the CJU now monitor the flow of documents between the BCU and FIB to ensure that relevant documents are being submitted within the correct time and to an appropriate standard. This is good practice, however, HMIC PNC Compliance Auditors were unable to determine how many other CJUs were carrying out this practice but they are aware that in another BCU, the practice of file management and document flows does differ.

2.1.7 HMIC PNC Compliance Auditors are of the opinion that whilst devolved management is effective for some aspects of policing, there is a need to provide a balance in certain areas to ensure that a corporate approach is maintained. This applies to the management of PNC which is a national system with statutory obligations concerning performance, therefore, in order to ensure that all risks are effectively controlled, a consistent approach is required.

Recommendation 1

Her Majesty's Inspector of Constabulary recommends that the force reviews the current level of management information being provided to BCU Commanders. The management information should ensure that individual officers can be held accountable for the submission and quality of the data being supplied. The force should also ensure that all BCUs are using the same information and that a corporate approach to accountability exists.

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 four 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 PNC Compliance 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 PsG and the overall management via the Bichard Information Management Board. The management of PNC is also included within the Business Plan for central Operations. However, whilst this provides the group with direction, HMIC PNC Compliance Auditors felt that there is a lack of specific strategic objectives that have been identified. For example, the force currently employs manual processes for the creation of A/S reports on the PNC but is currently considering the purchase of a system that will provide an interface between the force and PNC to speed up this process and provide a certain level of automation. Whilst the purchase is currently under consideration, there is no documented objective to state what outcome the force aims to achieve from the purchase, for example, whether the interface will transmit full or skeleton records and what impact this will have on current business processes

2.2.2.3 HMIC PNC Compliance Auditors are of the opinion that the force should develop a strategic action plan providing accountability upon individuals for the delivery of actions. The PsG should also have the action plan as a standing agenda item for future minutes to guarantee that actions are delivered in the appropriate time. The PsG can also ensure that all relevant factors that may impact upon the delivery of an action are considered by members of the group as the plan progresses. The plan should also be a dynamic document, with updates being made when new developments are introduced, for example, Schengen. Using the plan as a living document will place the force in a position where it is able to respond more effectively to changes.

2.2.2.4 With regards to force policy on PNC, HMIC PNC Compliance Auditors were pleased to note that the force has a wide range of policies covering the PNC functions. All policies are individually referenced and are available via the force intranet. They were also encouraged to learn that all staff are aware of the policies and where to find them.

Recommendation 2

Her Majesty's Inspector of Constabulary recommends that the force develops strategic objectives for the force, supplemented by a strategic action plan to ensure that progress towards the objectives can be monitored. The action plan should contain specific actions assigned to individuals who must be made accountable for the delivery of the actions.

2.2.3 Security

2.2.3.1 Under this section, HMIC PNC Compliance 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 managers and supervisors in the FIB and also by system administrators from the Information Services Department (ISD) support desk. Supervisors in FIB manage the user access of staff from FIB who are trained internally by accredited trainers. For all other staff, upon successful completion of a training course, individual forms are sent by the trainer to ISD. The forms are signed by the trainer and the trainee to ensure that the trainee is aware of their responsibilities on the system. Once the form is received by ISD, the relevant update to provide user access is carried out by placing the user in an appropriate user group.

2.2.3.3 When people leave the force, their details are included in General Orders, which is a weekly publication within the force containing information on new policies, changes to policy and other useful information as a reference. Staff in ISD also receive a download on a daily basis from the Human Resources (HR) system to ensure that user access is removed in a timely manner.

Recommendation 3

Her Majesty's Inspector of Constabulary recommends that in order to ensure independence of the complete process, all user access administration should be carried out by staff in ISD. The existing process that ISD use can be utilised by trainers in FIB to ensure staff are placed in the appropriate user groups.

2.2.3.4 However, whilst there is a process, HMIC PNC Compliance Auditors remain to be assured that user access has been managed effectively in the past and is in need of auditing to ensure that the current list is accurate and up to date. At the time of the inspection, the force had 4,050 user ID numbers for access to PNC, accounting for 80% of the whole workforce. A dip sample of 50 users has been carried out in the last twelve months but no feedback was provided to ISD staff regarding the accuracy of the information and no updates were made as a result of the sample audit. It is the opinion of HMIC PNC Compliance Auditors that a full audit of user IDs should be carried out to provide the force with assurance that the risk of misuse is minimal. There is an argument that once a person has left the force and the network access account is disabled, PNC access cannot be achieved. However, this does not prevent a current network user from using another PNC User ID to carry out PNC transactions because there is no link between network accounts and certain PNC applications, for example, S-Term which is a software emulation of a directly connected terminal.

Recommendation 4

Her Majesty's Inspector of Constabulary recommends that due to the high percentage of staff with a PNC user ID, a more detailed audit of user access to PNC is conducted to ensure all current user IDs are accurate and relevant.

2.2.3.5 General System Security is managed through Operation Minerva under the auspices of the security committee which is chaired by the Deputy Chief Constable. Operation Minerva is a strategic operation that ensures that all aspects of security have been taken into account in order that the force reduces the risks to it's information and other assets involved in processing the information. From the strategy, a comprehensive security policy has been produced in accordance with BS7799 and the ACPO Community Security Policy and is supported by individual System Operating Procedures (SOP) for each system including the PNC. In addition, staff are required to sign up to security matters before a network account is issued to them. This is considered to be good practice. An e-learning package is also being developed to provide further information and opportunities of training for all staff.

2.2.4 Data Protection

2.2.4.1 Data Protection sits within the Professional Standards Department (PSD) which falls within the portfolio of the DCC. This is good practice and ensures that the auditing regime remains independent of operational functions.

2.2.4.2 However, despite the organisational position of Data Protection being appropriate, HMIC PNC Compliance Auditors are of the opinion that the force is not realising the full potential that auditing can bring. Data Protection audits should provide assurance that the force is complying with the Data Protection Act and whilst recent audits contribute to this assurance, a number of weaknesses were found in the planning, execution and reporting of the audits.

2.2.4.3 The ACPO Data Protection and Audit Manual (DPAM) provides guidance on carrying out risk analyses of systems to assist in the development of an audit plan. The rationale is to ensure that audits are conducted against high risk systems and data. In Kent Police, the audit plan has been based upon a premise of cyclical audits, whereby there is simply a rolling programme of auditing in a sequence and when the sequence is complete, auditors return to the beginning and start over. There is currently no risk assessment conducted however, HMIC auditors were informed that this process is under review with a view to introducing risk based planning. HMIC Auditors support this review and would encourage the force to introduce risk based planning, with periodic reviews of the risk assessment to ensure that relevant systems are included in the plan.

2.2.4.4 In addition to the planning of audits, HMIC Auditors also found that recent audits against PNC data have been divisional based and not function based. With a national system like PNC, the force should be looking to gain assurance at corporate level that processes and data are complying with the act. If audits are divisional based, the audits will only identify weaknesses at local level and unless every division has a similar audit conducted, forcewide issues may not be identified. Thus, if there is a forcewide problem, there is a risk that it will not get addressed. Function based audits against particular aspects of the system, for example, an audit of the wanted/missing index, across the whole force would provide improved assurances for the force. Furthermore, HMIC Auditors are of the opinion that the force should consider the introduction of process based audits when measuring data protection compliance. The present format of audits is based upon vouching and verification of data and does not examine the business process behind the capture and maintenance of the data.

This means that whilst errors may be identified, opportunities to introduce more efficient or lower risk processes are being missed and the force is not gaining maximum benefit from the audit cycle. HMIC Auditors were informed that the consideration is being given to the introduction of process based audits and they support and encourage this move.

2.2.4.5 The lack of process based auditing is evident within the recommendations that have been made. HMIC Auditors felt that some recommendations lacked substance and were merely restating the control that should be in place. For example, in a recent audit of the originator line, where pro-formas were sent out to PNC operators who had conducted checks on the system, one of the findings related to the percentage of pro-formas that were returned within the prescribed period. The control is stated as;

"The Data Protection Unit require a response within a seven day period to ensure that all audits are performed within a designated time frame. This period was activated for return of pro-formas"

Within the report, the auditor comments on the percentage of forms that were retuned on time and the following recommendation was made;

"All staff must ensure they comply with the deadline for returning of pro-formas or to communicate reasons why they are unable to comply, with the auditor"

HMIC Auditors are of the opinion that had the audit been processed based, examination of the reasons for failure to comply could have been carried out. This would provide the auditor with improved knowledge when conducting audits in the future. The recommendation could also have then been written to reflect any areas of weakness that had been identified, for example, the involvement of local supervision in ensuring that pro-formas were returned. The 'Internal Audit – Originator Line' of July 2005 contains further examples of recommendations that could be improved with the use of process based auditing.

2.2.4.6 Finally, in relation to the format and quality of audit reporting, HMIC Auditors are concerned that there is no effective method of follow up when recommendations are made. A co-ordinator has responsibility for ensuring that recommendations are completed, e.g. that recommendations are assigned to somebody, however, HMIC Auditors were informed that no tracking is carried out to ensure that recommendations reach the point of implementation. In addition, the PsG is not provided with the results of audits reports relating to the PNC. This is partly due to the way that audits are conducted, e.g. Area based, therefore, the current responsibility rests with Area commanders. HMIC Auditors are of the opinion that the PsG should receive all PNC audit reports and should manage the implementation of recommendations through updates to the strategic action plan.

Recommendation 5

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

- **introduce risk based planning of audits in accordance with the ACPO Data Protection and Audit Manual;**
- **introduce function based audits of PNC to ensure that issues are addressed at force level as opposed to BCU level;**
- **initiate a change in the style of auditing from verification to process based auditing to provide opportunities to identify inefficiencies in processes that may be contributing to errors and omissions in the data;**
- **ensure that all PNC audit reports come under the ownership of the PNC sub-Group to guarantee that any recommendations are added to any action plans in order that progress can be monitored.**

2.2.4.7 HMIC Auditors also reviewed the process for transaction monitoring within the force. Transaction monitoring is a process contained within the 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.

2.2.4.8 In Kent Police, HMIC Auditors found that there is no rolling process for carrying out transaction monitoring. The force adopts an alternative method of carrying out an audit within the areas every six months. The audit is carried out against the originator line with pro-formas being sent to operators and enquirers in order for them to confirm the reasons for the transactions. The results form the basis of a formal audit report (see paragraph 2.2.4.5) However, due to the frequency of the checks being sent out, the process does not act as a deterrent for staff because they know that if they receive a verification form to complete, it is likely to be a number of months before another form is received. This provides staff with a "window of opportunity" to take a risk in carrying out transactions that are not for a legitimate policing purpose. It also means there is no immediacy in the checks, with staff receiving forms months after the transaction was carried out. Whilst it is force policy to endorse pocket note books for every PNC checks, officers and staff stated that in reality, it is often difficult to recall the reasons for transactions being made.

2.2.4.9 HMIC Auditors are of the opinion that in order to reduce the risk of misuse of PNC by staff in Kent Police, the force should introduce a process to carry out transaction monitoring on a continual rolling basis. This will also ensure that verification checks are current allowing staff an opportunity to recall the reasons for transactions.

Recommendation 6

Her Majesty's Inspector of Constabulary recommends that the Force should review the current process of transaction monitoring and introduce a rolling programme of transaction monitoring. A rolling programme will ensure that there is immediacy to the process and the random checks can be done without long breaks between staff receiving checks.

2.2.4.10 A positive outcome in terms of data protection is the level of training and information accesible to staff to raise awareness of their responsibilities. The e-learning package, known as 'Easy-Eye' that is available to promote Information Security, also includes aspects of Data Protection. The package continually assesses staff as they move through the training, assessments must be successful before further progress can be made. In addition, probationary constables receive a one hour input at week 6 of their initial training with police staff receiving the same input on induction courses.

2.3 People

2.3.1 PNC Awareness

2.3.1.1 HMIC Auditors were pleased with the level of knowledge of the PNC amongst officers and staff throughout the Force. The Force has undertaken marketing activity under the auspices of the PNC sub Group, including the development of a marketing strategy and the use of the Police Information Technology Organisation (PITO) to deliver presentations to raise the awareness of PNC as an investigative tool.

2.3.1.2 In addition, within the CID environment, PNC is widely used as an investigative tool by researches assigned to major investigations. The successful use of the researches has prompted the force to consider widening the access to VODS and QUEST to divisional based researches when a re-structure of the force is complete, reducing the number of Areas from nine to six. HMIC Auditors support this move to improve the availability of the PNC functionality.

2.3.1.3 Whilst there is good awareness amongst CID staff and some uniform staff, HMIC Auditors are of the opinion that the functions available to staff are not being used to their full potential. Staff reported that the process for obtaining more complex searches, for example, using VODS and QUEST, is bureaucratic and does not lend itself to real time investigations. (see paragraph 2.5.7.1). However, HMIC Auditors also learned that this perception is inaccurate as bureaucracy was avoided when necessary, therefore, there is a need to deliver this message to officers and staff to ensure they are aware of the true availability of all PNC functions.

2.3.1.4 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 during week 5 of the initial training, new officers receive a 3 hour session dedicated to PNC and the capabilities of the system.

2.3.1.5 HMIC Auditors were also pleased to note that the Force has an e-learning zone on the force intranet. This zone allows staff to browse the site and test their own knowledge in various aspects of policing. The e-learning zone has a section on the PNC in order that staff can test their own knowledge and improve their own levels of awareness of the functions available to them.

2.3.2 Training

2.3.2.1 PNC Training is available in the Force Information Bureau (FIB), the Force Communications Centre (FCC) and from the central IT training function within Information Systems Department (ISD). Training within FIB and FCC is a dedicated resource for their respective staff whilst ISD are responsible for training officers and staff from around the Force. The ISD training facility provides courses in PNC enquiry, FIB provides courses in enquiry, vehicle/property update, VODS and QUEST and FCC provides courses in enquiry and vehicle update.

2.3.2.2 Within the FIB, training is planned to coincide with the start date for new recruits to the office. The trainers provide PNC training in a classroom environment for one week, followed by a further two weeks on the job training on a one-to-one basis. Training courses are delivered depending on the section of the office where the new member of staff will be working, e.g. Arrest/Summons Input, court results or the 24 hour section providing operational support to officers. Courses within FIB do not have a formal assessment at the end because the trainers continually monitor the progress of new staff as the training is being delivered. Any shortfalls in knowledge can be addressed quickly because the trainer spends approximately three weeks with the new staff. The training is supported by mentors in the work place and all new staff have all of their work checked for quality with a feedback mechanism to training if issues are identified. All new staff are subject to a probationary period of six months with reviews every 3 months.

2.3.2.3 Within FCC, PNC training is provided as part of the six week training course that new operators receive. The first four weeks is classroom based which is when PNC training is delivered. PNC training consists of enquiry courses for names, vehicles and property and also update courses covering vehicle and property. The remaining two weeks is on the job coaching and mentoring. PNC training course within FCC do have an assessment attached to them, however, it is not carried out on a formal basis with a required pass mark that has to be achieved. The competence of staff is managed through on going assessments throughout the training and also through quality assurance checks carried out by FIB staff. Any update done within FCC is checked by FIB with feedback being provided to FCC supervision if issues are identified. Records of quality checks are kept and used to identify training needs if required.

2.3.2.4 The training provided by ISD trainers is planned twelve months in advance and provides approximately two courses each month. Places on courses are determined at local level through staff making request via the local management structure. ISD only provide enquiry level courses as all updates are carried out in FIB or FCC.

2.3.2.5 Similar to FIB and FCC, courses run by ISD are not formally assessed. Trainers continually assess students as they go through the course; however, this is not always done on an individual basis with students because in some cases, students are paired up at a terminal. The result is that without a formal assessment, the competence of the student is based upon the opinion of the trainer. The view of the HMIC Auditors is that all courses should be assessed in accordance with national guidelines. A formal assessment provides documentary evidence that students are competent in using the PNC. In addition, a formal assessment for course will enable an improved corporate approach to assessing PNC students. At present, the assessment process is different in FIB, FCC and ISD.

2.3.2.6 The varying levels of assessment also highlight the variation in the training that is being provided between the three sites. Without formal collaboration between each of the training departments, there is a risk of inconsistencies in the training being delivered. Therefore, the force would benefit from bringing all PNC training, where possible, in line with each other to ensure that a standard approach is being achieved, regardless of who delivers the training.

Recommendation 7

Her Majesty's Inspector of Constabulary recommends that formal assessments are carried out for all PNC courses to provide evidence of competency for all staff attending courses. The Force should also ensure that although training is directed to specific posts across the three training sites, the level of training is consistent across all three sites.

2.3.2.7 One area where consistency is achieved is the use of a Computer Based Training (CBT) package. The force has developed its own CBT package which has been approved by the Police Information, Communication and Technology Training Service (PICCTS). The package is completed by the student who must pass assessments at various stages of the package before progressing to further stages. At the conclusion of the package, students can print a certificate as proof of completion, however, PNC access is not granted until a further accreditation process has been carried out by a PNC trainer. The final accreditation is in the form of an assessment which students must pass in order to gain access to the system.

2.3.2.8 HMIC Auditors were impressed by the innovative approach, reducing the demand on time of the PNC trainers and also reducing the demand on classroom based courses. The CBT package also offers flexibility in the training as it can be carried out at the students own pace. HMIC Auditors are also of the opinion that other forces would benefit from such a package and would urge the force to consider marketing of the product to its colleagues.

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. Kent Police have taken the initiative in this area and developed a service level agreement (SLA) between itself and other agencies that prosecute offenders for recordable offences. The comprehensive, yet straightforward SLA ensures that non-police prosecuting agencies (NPPAs) are aware of their responsibilities for providing the force with information at the appropriate time. The SLA also allows provision for the sharing of data from the PNC with the NPPAs. The SLA is considered good practice by HMIC and the Kent model has also been used a number of forces throughout the country.

2.4.2 Furthermore, local senior management teams from the Areas have regular meetings with the local courts. The meetings deal with a range of issues but they are also a mechanism to ensure that the supply of data from the courts to the police, for timely updating of the PNC, is maintained and that any issues can be addressed if relevant. Whilst HMIC Auditors consider this to be good practice, they are not aware, or have been provided with evidence to suggest that when issues do arise, the PNC sub-Group is informed. HMIC Auditors are of the opinion that the PsG should ensure that any issues identified and discussed at local should be communicated to the group for information. This will ensure that chief officers and other senior managers can intervene or escalate matters to the Local Criminal Justice Board (LCJB) if required.

Recommendation 8

Her Majesty's Inspector of Constabulary recommends that the Force introduces a mechanism to ensure that any issues identified on a BCU relevant to the performance against PNC targets are highlighted to the PNC sub-Group.

2.4.3 Another area that HMIC Auditors reviewed under this protocol heading was the effectiveness of the force when attending regional and national PNC meetings. The force is currently actively involved in the South East, East & London Regional PNC Liaison Officers Conference and also represents the South East region on the P4G. These two roles ensure the force is suitably placed to respond to changes in policy and procedure or to become aware to changes in PNC functionality.

2.5 Processes

2.5.1 In terms of processes, HMIC PNC Compliance Auditors found a number of issues within Kent Police that are worthy of note in this report. These relate to the creation of Arrest/Summons reports, court results, data quality, MO keywording, ad-hoc intelligence updates, warrants and the originator line.

2.5.2 Creation of Arrest/Summons Reports

2.5.2.1 Within Kent Police, arrest/summons (A/S) reports are created initially as a skeleton record following a telephone call from the officer in the case. This process is known as the Verbal Arrest Summons (VAS). The full record is populated when the source input document, known locally as the 1837a is submitted in hard copy format to the FIB. This method has ensured that the force has been able to achieve the target, or close to the target on a consistent basis for initial entry of the record. However, despite the good performance, HMIC Auditors found a number of issues that the Force would be required to address to assist in improving the performance and maintaining it above the target figure of 90%.

2.5.2.2 During interviews and focus groups, officers informed HMIC Auditors that although they are aware of the need to telephone the initial details of an arrest to FIB, a number of comments were received to the effect that there is currently no accountability or responsibility for the supervision to ensure this has been done. In addition, there is no process at FIB to identify whether all cases have been submitted. This poses the risk that some cases will not be submitted to PNC and will only be identified when the offender appears at court, whereby the details of the case will appear on the court register. Without effective controls in place, the performance against the targets becomes difficult to sustain because identifying factors when under performance is encountered is not possible.

2.5.2.3 A similar issue exists concerning the submission of the 1837a forms. Officers are aware of their responsibilities for submitting the data in a timely manner and of the quality required, however, there is no effective process to ensure that an officer completes the form at the appropriate time. There is no local check made to ensure that a form is submitted for every telephone notification and FIB do not have the means to compare VAS records against source documents. The Force is currently piloting an electronic version of the form, to reduce the time taken for for a completed form to reach FIB, however, the same issues will exist with the e-form that currently exist with the manual form. The risk of this is that records could remain on the PNC in skeleton format without full details being appended to the record.

2.5.2.4 However, HMIC Auditors were informed that progress has been made in one Criminal Justice Unit to ensure that all forms are submitted. There is a CJU on each Area and they are responsible for the management of the case files when a new prosecution is taking place. In one Area, the CJU has been given the responsibility to ensure that an 1837a has been completed and submitted when they are reviewing the case files. If an 1837a does not exist, a request is made to the officer to submit the form and a record is kept of the failure. In view of the current manual process employed in Kent, HMIC Auditors consider this to be good practice, however, they are concerned that one Area is doing this in isolation and that the good practice has not been disseminated throughout the Force.

2.5.2.5 In making these observations, HMIC Auditors are aware of the Force plans to implement an electronic interface in the near future, superseding the need for VAS and potentially the 1837a forms. Whilst these specific issues may not be relevant, the principles behind them are, in that without effective processes and sufficient controls, the Force will remain at risk of under performance in the future.

Recommendation 9

Her Majesty's Inspector of Constabulary recommends that in conjunction with recommendation 1, the Force reviews the process for ensuring that all arrests, and subsequently, all 1837a's are submitted to FIB for the appropriate action. The process should include effective supervision at a local level. The Force should also consider the use of technology, for example Business Objects to provide FIB with a tool to monitor the custody system to ensure that all arrests are notified.

2.5.3 Court Results

2.5.3.1 Court results are updated by a specific section of FIB. An interface exists between the Equis system at the courts and Genesis, the local system within Kent Police. When a result is validated on Equis, an electronic message is sent to Genesis to alert staff that a case is ready to be updated onto the PNC. This process ensures that the supply of data from the courts should not hinder the force when striving to achieve the target of 75% of results within 10 days. However, at the time of the inspection, the force was not achieving the required target for input of court results,

2.5.3.2 HMIC Auditors reviewed the process for receiving court results and learned that at the moment, there is no corporate method of ensuring that all cases that are validated, have been notified to Genesis, therefore, the Force may be unaware that cases have failed to be transmitted. In one Area, the CJU, who have copies of the court agenda before the hearings start, carry out a comparative analysis between the court agenda and what has been received over the interface. This is good practice and ensures that where a transmission has failed, or is late, the CJU can take the matter up with the court as soon as possible. It was not made clear during the inspection whether all CJUs carry out this process, therefore, the Force may benefit from disseminating this good practice to ensure all court results are received.

2.5.3.3 In addition to court disposals, arrests that result in a refused charge at the custody suite can also impact on the performance of entering results. The Force has identified this as an issue and has found that not all refused charges are being notified to FIB within the required time. As a result, the Force has developed a process using Business Objects, a software package that can analyse data from various systems, to identify all refused charges on a given date. At the time of the inspection, this process was new, however, early indications from performance data is that the process is providing the required improvements.

2.5.3.4 With the success of Business Objects being used to analyse the existing custody system, HMIC Auditors suggest that the Force consider the benefits of the programme and it potential use to identify all cases that have been through custody that require an arrest/summons update onto the PNC. Use of the software in this way, could identify areas for improvement towards improved performance against the arrest/summons target. (see paragraph 2.5.2.2 and Recommendation 9)

2.5.3.5 Another area in which HMIC auditors found scope for improvement was in connection with the 1837a forms. If a result is received from the court, but an 1837a has not been received from the officer, the result is not updated. Staff from FIB chase up the 1837a and only when it has been received is the result added. This can also impact on the Forces ability to achieve the target for court results, therefore, if the issue of non-submission of forms is resolved (paragraph 2.5.2.3) there is scope for some results to be updated in a timelier manner.

Recommendation 10

Her Majesty's Inspector of Constabulary recommends that the current process in one BCU to monitor the deliver of court results is disseminated throughout all other BCUs. Once all BCUs are carrying out this role, management information should be collated to ensure that any consistent failures by the courts can be addressed at either local meetings between BCU Commanders and the courts or at a corporate level through the Local Criminal Justice Board.

2.5.4 Data Quality

2.5.4.1 Under this heading, HMIC Auditors considered the process for the quality assurance of updates to Arrest/Summons reports and court results, both of which are carried out in FIB.

2.5.4.2 Within FIB, supervisors have the responsibility to ensure that updates made by the staff are of a suitable standard. New staff have 100% of the work checked until they reach a standard whereby they are achieving 95% accuracy on a consistent basis. When 95% has been achieved, the proportion of work checked is reduced to approximately 10% for the court resulting team and 20% for staff who are updating A/S reports.

2.5.4.3 A spreadsheet is kept by the supervisor to record the results of the quality control checks. The spreadsheet is used to identify trends and is also used during staff appraisals. Each member of staff has an objective within the appraisal to achieve the appropriate standard of input. HMIC Auditors consider this to be good practice.

2.5.4.4 The existence of quality assurance work was evident during reality checks carried out by HMIC Auditors. Checks were made on the PNC against source documentation pertaining to A/S reports and court results. There were no significant errors found. A number of minor errors were detected, however, the scale of the errors would not have had any impact on the use of the information as they were classed as typographical errors.

2.5.5 MO Keywording

2.5.5.1 MO keywording is a process that provides a searchable database of MO data when conducting QUEST searches on the PNC. When offences are recorded on the PNC and a MO is provided, the Force selects keywords from the MO that might be relevant for future searches. Keywords can be the point of entry during a burglary, the age of a victim, the sex of a victim, location of offence or even the character assumed during a bogus official offence.

2.5.5.2 The current process for keywording is that the 1837a is used as the primary document for defining the keywords that are going to be updated on a particular A/S report. The force does not keyword every offence, however, it does target serious offences or cases which have an unusual MO. Specific staff are assigned to the task to ensure that knowledge and experience gained from the process can be used to develop improved keywording from limited data on the 1837a.

2.5.5.3 If insufficient information is provided on the 1837a, staff in FIB will make contact with the officer in case to ensure that further information is provided to enable the keywording to be done accurately, for the benefit of future QUEST searches. This is also considered to be good practice by HMIC Auditors.

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 Kent Police, the form 1837c, which is a supplementary form to the 1837a should be used to submit intelligence updates to local intelligence officers. If the intelligence is relevant for update to PNC, for example, a new address or a change in description, the form should be sent to FIB to enable the relevant update to be made to PNC.

2.5.6.3 During interviews and focus groups, HMIC auditors learned that the submission of the 1837c to FIB varied from Area to Area. Some Areas submitted the forms in accordance with the local force policy, while some officers stated that this did not happen on their Area. In view of this, HMIC Auditors are of the opinion that the Force should carry out some short term analysis to identify which Area are complying with the policy and which ones are failing in their obligations. Once the analysis has been conducted, the policy for submitting intelligence updates should be reinforced where weaknesses are identified.

Recommendation 11

Her Majesty's Inspector of Constabulary recommends that the Force should carry out short term analysis of the submission of ad hoc intelligence to identify any BCUs that are not complying with the policy. The Force should also reinforce the policy to ensure that all relevant data is captured and updated on to PNC.

2.5.7 VODS, QUEST and Transaction Enquiries

2.5.7.1 As previously mentioned in paragraph 2.3.1.3, there is a good awareness throughout the force of the investigative capabilities of the PNC. However, a number of officers informed HMIC Auditors that they are reluctant to make use of the facilities because the process is bureaucratic and does not allow provision for real time searches of the system when an urgent response is required.

2.5.7.2 The process for obtaining one of the more specialist searches on PNC is for the officer requesting the search to complete a form and submit it to the FIB via fax. The form requesting the search must also be signed by a supervisor before it is sent to FIB. Upon receipt of the fax, staff will conduct the necessary enquiries on behalf of the officer. The reason for the form to be completed is that if a search results in a positive hit, the details of the search criteria can be used as evidence during court proceedings

2.5.7.3 Whilst the perception amongst officers is that a form is required every time, FIB staff will carry out searches for urgent matters, recording details and asking officers to submit the form at a later date. This message needs to be communicated to all staff to ensure that the maximum potential of PNC is utilised when appropriate. The Force should also consider reviewing the process in order to remove the bureaucracy surrounding the checks. The onus on completion of a form for evidential reasons can be placed upon the operator when they are taking details of the request from the officer. As details are passed to the operator, the form can be completed and then the checks carried out, leaving the officer in the case free to conduct further enquiries. In addition, the removal of supervisory authority for the checks should also be considered to improve availability of the specialist searches.

Recommendation 12

Her Majesty's Inspector of Constabulary recommends that the process for requesting complex searches from PNC is reviewed. The current process is perceived as bureaucratic and is deterring officers from using the facilities. The Force should consider removing the need for a line manager to approve a request. The Force should also consider placing responsibility for recording the details of the request with FIB.

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, Kent Police do not update the PNC with any bail conditions, therefore, other forces will not always be alerted to the fact that conditions exist if they have originated in the Kent area.

2.5.8.2 Nevertheless, a scoping exercise is being conducted within the force to gauge the impact if the update of bail conditions was to start. HMIC Auditors support this exercise given that people from all parts of country pass through the county when using the ports within the Force as the gateway to Europe. The Force should consider the benefits that may be achieved if offenders from outside the Force area are given conditional bail and allowed to return to their own Force areas.

2.6 Results

2.6.1 In the 12 months to July 2005, Kent Police have maintained a consistent performance against the target for the creation of A/S reports. The force has consistently hit or fallen just short of the target of 90% in the five months leading up to the inspection. Between August 2004 and July 2005, the Force has achieved performance ranging from 85.9% to a high of 90.7% which was achieved in March 2005. During the same period, the volume of records created has increased by approximately 20% from 3,777 records to 4,496 records. With regards to the number of days taken to enter the quickest 90% of records, a similar consistent performance has been achieved with 2 days being the longest period over the last twelve months. Against both indicators, the force is performing better than the England & Wales averages of 82% and 11 days respectively.

2.6.2 Performance with regard to the input of court results has been less consistent. When the Code of Practice for PNC was introduced in January 2005, the force met the target of 50% in that first month. Performance dropped to 37.5% in March 2005, but has since improved 66.9% in July 2005. Whilst this remains outside of the revised target of 75%, the force has identified potential areas for improvement and is already taking remedial action to improve the overall performance. With regard to the number of days taken to meet the respective targets within the Code of Practice, 50% between January and June and 75% from July 1st, the Force has steadily reduced the number of days. In June 2005, it was taking 8 days to meet the target of 50%. In July 2005, it took the force 14 days to meet the new target of 75%, however, HMIC Auditors are satisfied that the remedial action mentioned above will address this drop in performance.

2.6.3 In terms of Impending Prosecutions (IPs), the overall number of outstanding IPs has increased from 9,545 to 11,734 between August 2004 and July 2005, an increase of approximately 23%. However, there is a direct correlation between the increase in the number of IPs and Kent's implementation of the 2003 Criminal Justice Act on 5th April 2005. 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. Each CJU receives a list of cases on a monthly basis to review. The results of the research carried out by CJU staff are returned to FIB in order that PNC can be updated accordingly.

Appendix A

A Summary of Good Practice within Kent Police

- All staff are required to sign up to the security policy before a network account is issued.
- The Data Protection function has a reporting line via the Deputy Chief Constable, providing independence to the process.
- BCU Commanders hold regular meetings with the courts providing an opportunity to raise issues affecting PNC performance.
- FIB staff have data quality as an objective within the appraisal system.
- If insufficient information is provided for MO keywording to be done effectively, officers are contacted to provide more information.

Summary of Recommendations for Kent Police

Recommendation 1

Her Majesty's Inspector of Constabulary recommends that the force reviews the current level of management information being provided to BCU Commanders. The management information should ensure that individual officers can be held accountable for the submission and quality of the data being supplied. The force should also ensure that all BCUs are using the same information and that a corporate approach to accountability exists.

(Paragraph 2.1.7)

Recommendation 2

Her Majesty's Inspector of Constabulary recommends that the force develops strategic objectives for the force, supplemented by a strategic action plan to ensure that progress towards the objectives can be monitored. The action plan should contain specific actions assigned to individuals who must be made accountable for the delivery of the actions.

(Paragraph 2.2.2.4)

Recommendation 3

Her Majesty's Inspector of Constabulary recommends that in order to ensure independence of the complete process, all user access administration should be carried out by staff in ISD. The existing process that ISD use can be utilised by trainers in FIB to ensure staff are placed in the appropriate user groups.

(Paragraph 2.2.3.3)

Recommendation 4

Her Majesty's Inspector of Constabulary recommends that due to the high percentage of staff with a PNC user ID, a more detailed audit of user access to PNC is conducted to ensure all current user IDs are accurate and relevant.

(Paragraph 2.2.3.4)

Recommendation 5

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

- introduce risk based planning of audits in accordance with the ACPO Data Protection and Audit Manual;
- introduce function based audits of PNC to ensure that issues are addressed at force level as opposed to BCU level;
- initiate a change in the style of auditing from verification to process based auditing to provide opportunities to identify inefficiencies in processes that may be contributing to errors and omissions in the data;
- ensure that all PNC audit reports come under the ownership of the PNC sub-Group to guarantee that any recommendations are added to any action plans in order that progress can be monitored.

(Paragraph 2.2.4.6)

Recommendation 6

Her Majesty's Inspector of Constabulary recommends that the Force should review the current process of transaction monitoring and introduce a rolling programme of transaction monitoring. A rolling programme will ensure that there is immediacy to the process and the random checks can be done without long breaks between staff receiving checks.

(Paragraph 2.2.4.9)

Recommendation 7

Her Majesty's Inspector of Constabulary recommends that formal assessments are carried out for all PNC courses to provide evidence of competency for all staff attending courses. The Force should also ensure that although training is directed to specific posts across the three training sites, the level of training is consistent across all three sites.

(Paragraph 2.3.2.6)

Recommendation 8

Her Majesty's Inspector of Constabulary recommends that the Force introduces a mechanism to ensure that any issues identified on a BCU relevant to the performance against PNC targets are highlighted to the PNC sub-Group.

(Paragraph 2.4.2)

Recommendation 9

Her Majesty's Inspector of Constabulary recommends that in conjunction with recommendation 1, the Force reviews the process for ensuring that all arrests, and subsequently, all 1837a's are submitted to FIB for the appropriate action. The process should include effective supervision at a local level. The Force should also consider the use of technology, for example Business Objects to provide FIB with a tool to monitor the custody system to ensure that all arrests are notified.

(Paragraph 2.5.2.5)

Recommendation 10

Her Majesty's Inspector of Constabulary recommends that the current process in one BCU to monitor the deliver of court results is disseminated throughout all other BCUs. Once all BCUs are carrying out this role, management information should be collated to ensure that any consistent failures by the courts can be addressed at either local meetings between BCU Commanders and the courts or at a corporate level through the Local Criminal Justice Board.

(Paragraph 2.5.3.5)

Recommendation 11

Her Majesty's Inspector of Constabulary recommends that the Force should carry out short term analysis of the submission of ad hoc intelligence to identify any BCUs that are not complying with the policy. The Force should also reinforce the policy to ensure that all relevant data is captured and updated on to PNC.

(Paragraph 2.5.6.3)

Recommendation 12

Her Majesty's Inspector of Constabulary recommends that the process for requesting complex searches from PNC is reviewed. The current process is perceived as bureaucratic and is deterring officers from using the facilities. The Force should consider removing the need for a line manager to approve a request. The Force should also consider placing responsibility for recording the details of the request with FIB.

(Paragraph 2.5.7.3)

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.