SUSSEX POLICE

13 – 17 DECEMBER 2004

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 Sussex Police between 13th and 17th December 2004.

1.1.2 Sussex Police was subject to a PNC Compliance Audit using the April 2003 Protocols on PNC Compliance. Her Majesty's Inspector would like to place on record her thanks to all members of staff who contributed to this report and provided assistance before and during the inspection.

1.1.3 This report is based on views and comments obtained from Strategic, PNC and customer level management and users at Force Headquarters, including HQ CID and at two of the six Basic Command Units (BCUs). These views have been supported by reality checks conducted by HMIC PNC Compliance Auditors.

1.2 Background

1.2.1 Sussex Police is a county force lying to the south of London and having the responsibility for policing the two counties of East and West Sussex. The force covers an area of approximately 4,800 square kilometres, serving a resident population of approximately 1.5 million. This number is significantly increased with seasonal visitors to the south coast holiday resorts, notably Brighton and Eastbourne. The counties of East and West Sussex provide a diverse range of policing challenges combining densely populated conurbations in some areas with a high number of rural communities. In addition, the force is responsible for policing services at Gatwick Airport, one of the busiest airports in the country handling over 30 million passengers a year.

1.2.2 Policing services within Sussex are provided by six BCUs, known locally as divisions; East Downs, Brighton & Hove, Hastings and Rother, West Downs, North Downs and Gatwick. The BCUs are sub-divided into a total of twelve districts providing local policing services with specific needs of communities.

1.2.3 The Force is headed by the command team comprising the Chief Constable, supported by a Deputy Chief Constable (DCC) and three Assistant Chief Constables (ACC) with individual responsibilities for territorial operations, specialist operations and operational support. There is also a civilian director of resources with overall responsibility for finance and administration. The Force strength comprises approximately 3,200 full-time equivalent police officers, 2,000 police staff and 155 special constables.

1.2.4 The PNC function falls within the portfolio of the ACC with responsibility for specialist operations. However, management of the function is devolved to a Superintendent as Head of CID, with day to day responsibility resting with the PNC Bureau Manager.

1.2.5 The PNC Bureau (PNCB) is responsible for all updates made to the PNC within Sussex Police including magistrates and crown court results, Wanted/Missing updates, Vehicle and Property Reports and full update of Arrest/Summons information. The bureau also provides an enquiry service for officers requesting PNC information via a telephone, either from landline or the telephony service available through the Airwave radio system. In addition, the PNC bureau is also the central point of contact for conducting Vehicle On Line Descriptive Searches (VODS) and Queries Using Enhanced Search Techniques (QUEST).

1.2.6 The PNCB is based within Sussex House, an office building on the outskirts of Brighton occupied by HQ CID. The bureau is staffed 24 hours a day, 7 seven days a week operating a rota of five shifts with four staff per shift. The shift system covers the hours of 7am – 5pm (days), 2pm – Midnight (Lates) and 11pm – 7am (nights).

1.2.7 Arrest/summons records are created manually by the PNCB following receipt of the necessary information from the custody system, known as CEDAR. When an offender is brought into custody, the custody sergeant or a civilian detention officer (CDO) completes initial details on the custody record. The officer in the case is responsible for completing a section of the custody record known as the PNC1, which contain more in-depth information about the offender. Once the custody sergeant or the CDO closes the custody record, the information is sent in the form of an e-mail to the PNCB in order for the record to be created on the PNC.

1.2.8 Magistrates court results are updated following receipt of information from the courts electronically, via an innovative link between the magistrates courts' system and the Sussex Police intranet. When a case has been validated by the courts, the information is sent on a case by case basis to a specific location on the force intranet where the results are reviewed by staff in the PNCB and updated onto PNC. The receipt of Crown Court results remains a manual process with hard copies of the results being sent from the Crown Courts to the PNCB.

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 area 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 HMIC PNC Compliance Auditors visiting the force and 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 records and court results.

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 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 targets set by the PIs in order to improve their position for each of the aspects mentioned above. The key PIs of the strategy are as follows: -

i. Arrest/Summons – 90% of cases to be entered within 24 hours (where forces are using skeleton records as initial entry, full update must be achieved within 5 days)
ii. Bail Conditions – Entry of Police Bail within 24 hours
iii. Court Case Results – 100% to be entered within 72 hours of coming into police possession. (Courts have their own target of three days for the delivery of data to the police, therefore, the police are measured against an overall target of 7 days, to take account of weekends and bank holidays)

1.4.4 At the time of the inspection, the standards for timely entry of data to PNC were subject of imminent change. 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.

1.4.5 There is a new PNC Code of Practice to be introduced on 1st January 2005, developed by Centrex and endorsed by ACPO is a statutory code made under S.39a of the Police Act 1996 (inserted by section 2 of the Police Reform Act 2002). It provides scope for the Home Secretary to invoke statutory intervention for forces failing to comply the code. Whilst the penalties for non-compliance are more severe, the standards within the code, particularly those that are affected by non-police agencies have been made less stringent.

1.4.6 The revised timeliness standards within the code of practice 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 on to PNC within 7 days of the information being received by the police. This target will be increased to 75% six months after the commencement of the code.

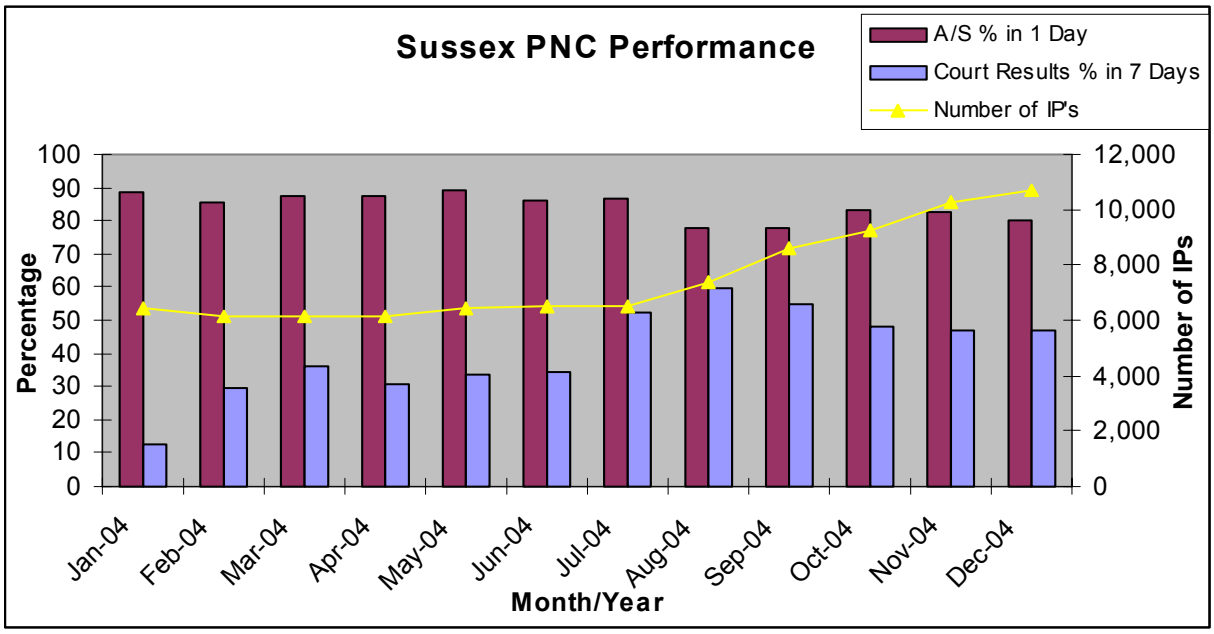
1.4.7 In view of the changes to the timeliness standards, this report will provide judgement on current performance that applied to the ACPO Compliance Strategy which was in effect at the time of the inspection. The report will also provide information on how the force is performing against the new code of practice to enable the force to determine the level of work that may still be required.

1.4.8 Sussex Police have experienced a slight decline in performance over the last twelve months with regards to the creation of Arrest/Summons reports. In January 2004, 88.5% of reports were created within 24 hours, rising to a peak of 89% in May 2004, just outside of the target. However, in September 2004 only 77.8% of reports were created within 24 hours rising slightly to the latest figure of 80.1% in December 2004. This latest performance is currently below the standard required within the new code of practice. In terms of the number of days to enter the best 90% of records, performance has remained consistent over the last twelve months. In January 2004, 90% of cases were taking 7 days to be created on the PNC, this improved to 2 days in May 2004 but the latest statistics available show that in December 2004, performance had slipped slightly to 6 days.

1.4.9 A similar trend is also evident in relation to the update of court results. In the first six months of 2004, significant improvements were made in the percentage of cases entered within the target time of 7 days, however, this has declined slightly in the final quarter of the year. In January 2004, 12.4% of court disposals were updated on PNC within 7 days, rising to 59.7% in August 2004. However, latest data shows that only 47.1% of cases were input within the target time, meaning that the force is not achieving the standard required within the new code of practice. In terms of the number of days to achieve 90% of cases, performance has also declined overall in the last twelve months. In January 2004, it was taking 56 days to enter the quickest 90% of cases, this figure improved to 20 days in February 2004, but has since declined further to 78 days in December 2004.

1.4.10 With regards to Impending prosecutions, Sussex Police have experienced an increase of 68% in the total number of outstanding cases on PNC from 6,402 in January 2004 to 10,733 in December 2004. Part of this increase can be attributed to the force commencing with a process to record all offenders at the commencement of proceedings, for example, those subject to Sec.47(3) Police Bail. This new process has resulted in a monthly increase of 57% in the cases being created on PNC by Sussex Police. The increase in the number of cases will eventually level out and the current process of using lists of old cases to enable review by Criminal Justice Units should ensure sufficient management of the overall numbers. Nevertheless, the force should maintain continual monitoring of the numbers to ensure that it can satisfy itself that the situation is being effectively managed.

1.4.11 A graph illustrating Sussex Police's performance in the 12 months to December 2004 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 in 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:

- Her Majesty's Inspector of Constabulary is pleased that the force has taken the initiative to develop a new system with an interface to the courts to improve the timeliness of court results. However, despite significant improvements being made, the full potential benefits of the system are not being realised.
- There is currently no formal strategy for the long term management of PNC and there is a lack of up to date or comprehensive PNC policy documentation.
- There are concerns that limited Data Protection Audits have been conducted in the last twelve months. In addition, there is no risk based audit plan for the management of audits and the capacity of the Access to Information Team will place further limitations on the number of audits being conducted.
- Transaction Monitoring is not being carried to the required level.
- There is also a concern regarding the level of training being provided to officers to enable access to PNC via Mobile Data Terminals. Efficiency savings available from this technology are not being realised due to the level of training being provided. Concerns also exists regarding the sharing of passwords amongst untrained users.
- The level of accountability of officers submitting data to PNC is limited. BCU Commanders are not provided with management information to tackle issues that may exist with their officers. .

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 At the time of the inspection, there had been a change in terms of leadership within Sussex Police. The portfolios of the Assistant Chief Constables (ACC) had changed resulting in a different ACC holding the responsibility for the PNC. However, the current ACC has a good awareness of the issues surrounding the PNC.

2.1.2 The force has an established Steering Group for the strategic management of the PNC. Historically, the steering group was a PNC Steering Group, but due to the co-location of CID, Force Intelligence and PNC and the overall management structure of these three areas, the group was reformed as the Intelligence Steering Group (ISG) in May 2004. The new ISG meets on a regular basis and has always been chaired by a chief officer. If a chief officer is not available, the meeting is postponed until such a time when the chief officer is available. HMIC PNC Compliance Auditors are satisfied with the approach of chief officers and the structure of the group, however, they do suggest caution concerning PNC to ensure its profile is maintained within the terms of reference of the group.

2.1.3 Whilst HMIC PNC Compliance Auditors are pleased with the structure and membership of the group, containing a broad spread of relevant staff from across the force, they were disappointed to note that some members consistently send apologies for the meeting without sending a replacement.

2.1.4 With regard to overall force performance against the targets of the ACPO Compliance Strategy for PNC, performance is monitored continually by the PNC Manager but Divisional Commanders only receive the information on a quarterly basis when the PNC Quarterly report is published by the Police Information Technology Organisation (PITO). A suite of performance information is produced on a monthly basis and published on the force intranet, however, PNC performance does not form part of this suite of information. In view of the inclusion of PNC performance within the Police Performance Assessment Framework (PPAF) from March 2005, HMIC PNC Compliance Auditors recommend that the force considers the inclusion of PNC performance in the future.

2.1.5 In addition, divisional commanders are not made aware of the quality and timeliness performance from officers under their command, when submitting data for update to PNC. The force operates a custody system in which custody suites are aligned to criminal justice department rather than the BCU. For the purpose of monitoring quality and timeliness information, a database (known locally as the Errors Database), is managed and populated within the PNCB, however, the data recorded is broken down by Custody area and not BCU. The result is that BCU commanders cannot hold their officers accountable because they are not provided with suitable management information. In addition, the database does not go into suitable depth when reporting information. For example, it will show the number of poor submissions for a particular custody suite but it cannot provide information whether the recorded number is of significant concern, e.g. the percentage of poor

submission against the overall number of submissions. Whilst this weakness in the system is evident, HMIC PNC Compliance Auditors recognise the innovation in commencing with the development of a system to record this type of information. Nevertheless, HMIC PNC Compliance Auditors recommend that the reporting from the system is reviewed to ensure that suitable management information is available to BCU Commanders and Custody managers alike, increasing the accountability placed upon officers.

Recommendation 1

Her Majesty's Inspector recommends that in order to improve the level of management information available to BCU Commanders and custody managers, thus increasing accountability of officers, consideration should be given to upgrading the reporting function of the 'Errors Database'.

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 Strategy, PNC Policy, Data Protection and Security. Each of these themes is discussed in further detail below.

2.2.2 PNC Strategy

2.2.2.1 In HMIC's Second Report on the Police National Computer Data Quality and Timeliness (the recommendations of which are provided in Appendix E of this report), it was recommended that a PNC Strategy should be an integral part of the Force's Information Management Strategy. HMIC PNC Compliance Auditors learned that at present, Sussex Police do not currently have either a documented PNC Strategy or a strategic action plan to maximise their use of PNC and ensure continued improvements in performance.

2.2.2.2 The terms of reference for the ISG provide scope for the strategic management of PNC, however, with no short, medium or long-term strategic aims, the force is reactive towards changes and external influences in relation to PNC. A strategy would provide a framework to examine ways to maximise the force's use of PNC and also ensure that the force takes a proactive position and is able to respond to changes more effectively.

2.2.2.3 Whilst there is no documented strategy, HMIC PNC Compliance Auditors were provided with a copy of the Operations/Intelligence Branch Performance Plan for 2003-2004. This document set out aims and objectives for the branch including provision for improvements to PNC performance and availability, but only in the areas managed within the branch. A formal PNC Strategy would remove the isolated approach of dealing with specific PNC issues and enable the force to adopt a holistic approach, overseen by all members of the steering group.

Recommendation 2

Her Majesty's Inspector of Constabulary recommends that the force develop a strategy for PNC in order to meet the short, medium and long-term demands of the system. Any strategy should include provision for future developments to the system, procedural impacts and marketing of changes to all relevant personnel.

2.2.3 PNC Policy

2.2.3.1 HMIC PNC Compliance Auditors found that there is a lack of comprehensive policy documentation supporting the use and availability of PNC within Sussex. There are individual policies for certain aspects of the system, but these are out of date and are in need of updating. For example, the policy for the Completion and Submission of information to PNC dates back to 2001 and still refers to a hard copy document known as the C-55. This document has been superseded by an electronic version known as the PNC1 but the policy has not been updated to reflect the change. In addition, during focus groups and interviews, many staff were not aware of the existence of any up to date policies.

2.2.3.2 Clear defined policies are essential to ensure that all staff are aware of their responsibilities when using the system. Policies should provide guidance and information on all aspects of PNC covering each application and taking account of the full range of updates, for example, arrest/summons updates, warrants, vehicles, property and the investigative use of the system. The existence of policies also enables the force to make staff accountable for their actions and inform them of any penalties for acting in breach of force policy. Any discipline cases that may arise could be conducted against the benchmark laid down in force policy and therefore, become easier to administer and gather evidence.

2.2.3.3 At the time of the inspection, HMIC PNC Compliance Auditors were informed of plans to develop a PNC policy under the auspices of the ISG. HMIC PNC Compliance Auditors welcome this move and recommend that the development of the policy is given a high priority and that all aspects of PNC use, including the timeliness and quality of data submitted for update to PNC, are covered within the document.

Recommendation 3

Her Majesty's Inspector of Constabulary recommends that the force continue with its plans to develop a PNC policy, consolidating and updating all existing policies. The development and publication of the policy will ensure that all staff either using or updating PNC data are aware of their responsibilities.

2.2.4 Security

2.2.4.1 The force has an Information Security Management Board (ISMB), chaired by the Director of Finance and Administration, which has responsibility for general IT security issues within the force. The group is also responsible for endorsing the Force Information Security Policy (FISP) and approving its publication. During the inspection, HMIC PNC Compliance Auditors were provided with a copy of the first FISP to be published within force. The current version is yet to be ratified by the ISMB, therefore it is not a published document. Nevertheless, HMIC PNC Compliance Auditors were pleased to note that the document has been developed in accordance with BS7799 and the ACPO Community Security Policy.

2.2.4.2 In addition to the FISP, the ISMB is responsible for promoting information security amongst all staff within the force. HMIC PNC Compliance Auditors were also pleased to learn that this has resulted in all induction courses and Stage 1 Probationer courses containing an input regarding information security. In addition, all IT training courses include an input on information security and trainees from IT courses are required to sign a statement stating that they are aware of their responsibilities concerning information security. HMIC PNC Compliance Auditors consider this to be good practice.

2.2.4.3 In terms of security of the PNC, HMIC PNC Compliance Auditors reviewed the structure of the user access groups and the processes employed in managing the setting up and maintenance of the groups. The management of the groups and access to PNC is managed by the PNC Liaison Officer (PNCLO) in the PNC Bureau.

2.2.4.4 The force is undergoing a change in connectivity from standard interface to a web based solution. The introduction of the web based solution has enabled the force to manage user access more effectively and tailor the structure of the groups to specific needs. In order to gain access to PNC via one of these groups, the PNCLO must receive notification from an accredited PNC trainer that a trainee has successfully completed a training course. This ensures that only staff trained to the correct standard will receive access to the system.

2.2.4.5 The PNCLO is also responsible for reviewing the user IDs contained within the groups to ensure they are relevant and up to date. Routine Orders published on a weekly basis contain information regarding staff who have left the force or who have changed roles. The PNCLO reviews this list and makes the necessary changes to the groups accordingly. In addition, on a periodic basis, the PNCLO conducts a review of all users IDs to identify staff who have not used the system over a three month period. Any staff identified through this process are contacted concerning their future access to the system.

2.2.4.6 However, HMIC PNC Compliance Auditors are concerned regarding the level of control applied to access to PNC via a mobile data terminal (MDT). Paragraph 2.3.2.6 provides more detail concerning MDTs, however, HMIC PNC Compliance Auditors felt that one aspect is worthy of note under the broad heading of security. During interviews and focus groups, anecdotal evidence was provided stating that passwords for MDTs are often shared and that access to the system has been provided to staff on the basis of a telephone call to the system administrator. As MDTs provide access to PNC, HMIC PNC Compliance Auditors are of the opinion that control of access should be administered to the same level as if access was being provided by a desktop computer. All staff should receive appropriate training and system administrators should be in receipt of a specific notification to enable the setting up of a new user.

Recommendation 4

Her Majesty's Inspector of Constabulary recommends that the force urgently reviews the administration process surrounding the access control to PNC via Mobile Data Terminals. System administrators should be in receipt of an authorisation prior to granting access to new users. In addition, the force should reinforce the Information Security Policy concerning the control of passwords on IT systems.

2.2.5 Data Protection

2.2.5.1 The data protection function is carried out by the 'Access to Information' Team. The team is managed by the Information Compliance Manager whose responsibilities include those that are traditionally related to a Data Protection, as well as having responsibility for Freedom of Information (FOI) within the force. In addition, there is a disclosure officer plus one assistant for dealing with subject access requests, one auditor and one FOI implementation clerk.

2.2.5.2 At the time of the inspection, there was no risk based audit plan covering the IT environment within Sussex, including the PNC. During the calendar year of 2004, only one audit had been completed which was a full audit of registered sex offenders. This audit included an audit of the PNC related data and took approximately 9 months to complete. HMIC PNC Compliance Auditors are of the opinion that the force should urgently consider the development of a risk based audit plan that is achievable and will provide assurance to the force concerning the data that it owns. The development of an audit plan is also a requirement of the new code of practice for the PNC.

2.2.5.3 Although the level of auditing has been limited over the past year, HMIC PNC Compliance Auditors were provided with a copy of a report produced by the Access to Information team. The report was structured in accordance with the format of the ACPO Data Protection and Audit Manual (DPAM), including the classification and identification of errors. HMIC PNC Compliance Auditors were also informed that reports are published to the Information Quality Board (IQB), a group chaired by the Deputy Chief Constable (DCC). The IQB are responsible for ensuring that all recommendations are followed through to completion. However, HMIC PNC Compliance Auditors are concerned that there is no direct link between the reports

pertaining to PNC and the Intelligence Steering Group. The ISG should take ownership of PNC related issues resulting from a Data Protection Audit.

2.2.5.4 In addition to data protection audits, the Access to Information team are also responsible for conducting transaction monitoring across the force. The DPAM states that forces should conduct a minimum of three transaction checks per day. However, whilst Sussex Police have a target of conducting 6 checks per day, by December 2004, only 193 checks had been carried out in the previous 12 months, falling well short of the required level.

2.2.5.5 Nevertheless, despite the need for increases in the volume of checks, HMIC PNC Compliance Auditors are satisfied that the process employed to conduct the checks is adequate. An e-mail is sent to the person requesting a check, who must respond via their line supervisor, giving reasons for the PNC enquiry being made. When responses are received by the Access to Information team, the reasons provided, for example, an incident number, are verified. For checks where a reason provided is not valid, the Information Compliance Manager can use an escalation procedure to have the matter investigated by the Professional Standards Unit.

2.2.5.6 In addition, during interviews and focus groups, all staff were aware of the process for transaction monitoring and were aware of the reasons why checks are carried out. Also, all staff were of the opinion that the process is a deterrent against misuse of the system. However, HMIC PNC Compliance Auditors were informed that a proposal to move responsibility for transaction monitoring to PNCB is under discussion. HMIC PNC Compliance Auditors are of the opinion that by going ahead with this, independence of the process will be lost as staff with operational responsibility for PNC will be conducting the checks. This could result in one member of staff within PNCB requesting validation of a check from one of their own colleagues. It is the view of HMIC PNC Compliance Auditors that the process should remain within the Access to Information team.

Recommendation 5

Her Majesty's Inspector of Constabulary recommends that;

- **the force considers the level of resources assigned to the Access to Information Team to ensure that a sufficient assurance can be gained from the activities conducted by the team.**
- **in order to comply with the code of practice for PNC and to gain assurance concerning the data that is being processed within force, the force should urgently consider the development of a risk based audit plan covering all IT systems.**
- **the force should also ensure that PNC related matters resulting from Data Protection Audits are 'owned' by the Intelligence Steering Group to ensure an effective follow up.**
- **The force retains the process for transaction monitoring within the Access to Information team and increases the number of transaction monitoring checks conducted on a regular basis.**

2.2.5.7 Finally in relation to Data Protection, HMIC PNC Compliance Auditors were pleased to learn that Data Protection training is provided to all new staff, during probationer courses for new officers and induction courses for new police staff. All IT courses also include a section covering this topic, so that staff using the force IT infrastructure are aware of their responsibilities. HMIC PNC Compliance Auditors consider this to be good practice.

2.3 People

2.3.1 PNC Awareness

2.3.1.1 The level of awareness of functionality that PNC offers varied across the force, particularly between uniformed police officers and officers within the CID environment.

2.3.1.2 The co-location of staff from the PNCB, Force Intelligence and CID has led to a high level of awareness of PNC functionality amongst Intelligence and Operations staff. Staff considered as CID staff were aware of the investigative capabilities of PNC, through the use of VODS and QUEST, with these transactions being included as part of routine research, for example, when a Major Crime Team (MCT) had been formed to investigate a serious crime.

2.3.1.3 With regards to uniformed staff and other officers working from BCUs, the level of awareness was variable. During interviews and focus groups, HMIC PNC Compliance Auditors received mixed comments from officers. In some cases, the response was positive concerning the communication of new functionality, however, in some cases, officers stated that they had not heard of certain applications, even though they have been available for over 5 years, e.g. some officer were not aware of VODS which was introduced in 1997.

2.3.1.4 The inconsistencies concerning the knowledge of PNC is further evidenced by the update of relevant intelligence on PNC. Intelligence submissions by officer are made on a form known as the C22. The divisional intelligence unit (DIU) is responsible for analysing the submission and providing a rating under the 5x5x5 rating system. If the data is relevant to PNC, the form can be sent to the PNCB for update to PNC. However, PNCB staff confirmed that the receipt of C22 forms was sporadic and that whilst some forms are received from certain BCUs, other BCUs do not send any updates to them. Due to time constraints during the inspection, HMIC PNC Compliance Auditors were unable to verify whether this was a lack of knowledge within the DIU or not, however, it was the perception of the PNCB staff and therefore, an area that the force may wish to examine.

2.3.1.5 The lack of a formal communication strategy for PNC has resulted in many officers learning about the system through ‘word of mouth’. Whilst this method can produce positive results amongst closely knit teams, it also carries the risk that messages become diluted and officers do not receive sufficient information. HMIC PNC Compliance Auditors are aware that the PNC Manager and PNCB staff distribute changes via e-mail and Routine Orders to PNC users. In addition, the force newspaper, ‘Patrol’ has also been used, however, in many cases, the message does not reach the operational officers. A lack of knowledge concerning the functionality of PNC can lead to missed opportunities for the force if officers are unaware of what

searches can be carried out. The force, when considering its strategic position in relation to PNC (see Recommendation 2), should also make provision for a structured approach to marketing of the PNC.

2.3.1.6 Whilst awareness was low amongst officers, HMIC PNC Compliance Auditors received many positive comments from officers regarding the PNCB and staff in the two control rooms, known locally and the North Resource Centre and South Resource Centre (NRC/SRC). All officers stated that operators had expert knowledge of PNC and often prompted officers to consider alternative lines of inquiry based upon what PNC had to offer. Whilst this assists in closing the knowledge gap amongst operational officers HMIC PNC Compliance Auditors are of the opinion that police officers should be aware of what is available to them, so that they can conduct inquiries in an efficient manner.

Recommendation 6

Her Majesty's Inspector of Constabulary recommends that as part of the development of a PNC Strategy (see Recommendation 2), the force develops a marketing strategy to raise awareness of PNC functionality amongst all staff.

2.3.2 Training

2.3.2.1 PNC Training within Sussex Police is available from either the force training school, a dedicated trainer within the PNCB, or by divisional staff when training officers in the use of Mobile Data Terminals (MDTs).

2.3.2.2 The force training school has two accredited PNC trainers who can deliver a range of modular based enquiry courses. Courses are planned in six month cycles by the training manager and candidates must make an application for a place on a course. The application must be linked to an objective within the candidates Performance and Development Review (PDR) and be validated by local Human Resources (HR) managers before contact is made with the training school. HMIC PNC Compliance Auditors consider this to be good practice to ensure that time available for training is maximised, by training only those staff who have a requirement to use the system.

2.3.2.3 In addition, HMIC PNC Compliance Auditors were pleased to discover that all training courses delivered by the force training school are assessed as a pass or fail course. Candidates must achieve a mark of 75% to ensure they pass the course and obtain access to the system. If a candidate fails the course by a significant margin, they must complete the course again, however, if the failure is considered to be borderline, the trainer will make a judgement and offer guidance and support to the candidate in areas of weakness. Furthermore, the force training school also conducts post training evaluation of courses to ensure that whilst courses are meeting the appropriate national standard, the content and delivery is meeting the needs of the candidates. Post training evaluation consists of ‘happy sheets’ that candidates complete at the end of the course, followed up two weeks later by the training school contacting the line manager of the candidate to obtain further

feedback once the candidate has used their new skills in the workplace. HMIC PNC Compliance Auditors also consider this to be good practice.

2.3.2.4 However, whilst HMIC PNC Compliance Auditors found good practice regarding the delivery of courses in the force training school, they are concerned with the lack of resilience within the training school. Currently, there are two accredited PNC trainers within the school, but at the time of the inspection, both trainers were working on other long term projects. The result of this abstraction is that no PNC training was being offered for a period of up to six months, increasing the potential for unworkable demand in the future.

2.3.2.5 HMIC PNC Compliance Auditors learned that some of this demand has been dealt with through the use of the PNC trainer from the PNCB. The PNCB trainer is also an accredited PNC trainer but also provides general IT training to PNCB staff. The main purpose of the role of the trainer within PNCB is to ensure that all staff are fully up to date with functionality on the PNC and other IT systems within force. The trainer is located within PNCB, therefore, there is increased flexibility on the delivery of training and there is no waiting time for staff who may require the training. However, HMIC PNC Compliance Auditors discovered that the trainer has been used in the past to deliver courses that would otherwise have been provided by the force training school. The training was provided by the trainer working overtime to meet the demand, therefore, confirming the lack of resilience within the training school and identifying the extra costs involved as a result.

Recommendation 7

Her Majesty's Inspector of Constabulary recommends that in light of the secondment of PNC trainers to long term projects, the force consider its position concerning the delivery and availability of PNC training.

2.3.2.6 PNC training is also available to staff via a training course aimed at new users of MDTs, however, this is an area of concern for HMIC PNC Compliance Auditors. MDTs offer an opportunity to provide efficient and secure use of data by officers who are out on patrol. The concept is that officers do not have to contact one of the resource centres to obtain information, hence there is no use of an operator's time and no information is being broadcast via the radio. In Sussex, the force has embraced this technology and has provided officers with access to numerous systems and databases, including the PNC. However, HMIC PNC Compliance Auditors are of the opinion that the force is not achieving maximum efficiency of the PNC via the MDTs.

2.3.2.7 The training course for an MDT is approximately half a day. This time includes an overview of the equipment and the use of the various applications available on the equipment. Divisional training staff delivers the training and there is no requirement for them to be PNC trained before training others to use the MDTs. There is also no assessment conducted prior to access being granted to new users. In contrast, regular PNC courses must be delivered by accredited PNC trainers, there is an assessment to ensure that candidates have achieved a sufficient standard and there are national standards for the delivery of courses.

2.3.2.8 Whilst HMIC PNC Compliance Auditors acknowledge that there are no standards for the delivery of PNC training for MDTs, the principles concerning access to PNC should be maintained. The current training has an emphasis on the use of the equipment, however, HMIC PNC Compliance Auditors are of the opinion that in terms of PNC, the emphasis should be on the interpretation of the data. If users are not trained adequately, there is a risk that a user can misinterpret data so that the perceived efficiency savings are not gained. Anecdotal evidence was provided by PNCB staff and resource centre staff that when officers conduct a PNC check on an MDT, they often still carry out a radio or telephone check to obtain clarification. This evidence highlights the weakness in the training.

2.3.2.9 It is the view of HMIC PNC Compliance Auditors that the PNC aspect of the training for MDTs should conform, where possible to existing national standards. A new standard has been developed for PNC access via Airwave and the force may benefit from using this as a model of good practice for the delivery of training where PNC is accessed from a remote device.

Recommendation 8

Her Majesty's Inspector of Constabulary recommends that the force urgently considers the quality and delivery of training for PNC access via Mobile Data Terminals. The training should be of a measurable standard and where possible, comply with national standards.

2.4 Partnerships and Resources

2.4.1 The force has developed a strong relationship with the magistrates' courts resulting in the development of a system that receives court information electronically. The development of the system has been a combined effort and whilst the performance of court resulting has not achieved the national targets, the system has provided significant performance improvements since it was introduced. In addition to the relationship between the courts, the force has a record of regular meetings between the Criminal Justice Department (CJD) and the Court Managers, in order to improve communication and performance. This is considered to be good practice, however, HMIC PNC Compliance Auditors learned that the meetings between CJD and the Court Managers have not taken place for a few months. The force should consider refreshing this area as an avenue to raise any issues that may be preventing the force from continuing with improved performance.

Recommendation 9

Her Majesty's Inspector of Constabulary recommends that the force reintroduce the meetings between Criminal Justice staff and the Magistrates Courts. The meetings should also involve a representative from the PNCB management team to ensure that issue affecting performance can be raised pursued.

2.4.2 In addition to good relationships with the courts, the force has also developed good lines of communication between itself and Non Police Prosecuting Agencies (NPPAs). A service level agreement (SLA) has been produced outlining the responsibilities of the NPPAs when supplying information for the PNC and also the responsibilities that the police will undertake when providing previous convictions to the NPPAs. The result of the SLA is that timeliness regarding the submission of data from NPPAs has improved. Data is either sent manually through the post or electronically via e-mail. Anecdotal evidence obtained during the inspection was provided to indicate the SLA is meeting it's aims of improving performance.

2.4.3 HMIC PNC Compliance Auditors consider this aspect of the report to be an area of strength for the force.

2.5 Processes

2.5.1 HMIC PNC Compliance Auditors reviewed the following processes within Sussex Police; Creation of Arrest/Summons Reports, Data Quality, Court Results, Ad Hoc Intelligence Updates and the PNC Bureau.

2.5.2 Creation of Arrest/Summons Reports

2.5.2.1 Sussex Police are one the few remaining forces who create Arrest/Summons reports on the PNC manually. The process is supported by a certain degree of automation between the custody suites and the PNCB but all updates to PNC are manual.

2.5.2.2 When an offender is arrested or brought into custody, the custody officer, or a civilian detention officer, create a new custody record on the custody system. Within the custody system, there is an electronic form, known as the PNC1 form, containing descriptive information about the offender, that is completed by the officer in case whilst the offender is still within the confines of the custody suite. The custody record cannot be closed until the PNC1 form has been completed. When the custody record is closed, the PNC1 is automatically sent to an e-mail address within the PNCB to enable the prompt input of the information to PNC.

2.5.2.3 HMIC PNC Compliance Auditors are satisfied that in the absence of an interface between the custody and PNC, the overall process is robust enough to continue to provide the force with continued performance. This robustness has already been proven following the decision by the force to input police bail and penalty notices for disorder onto the system. The decision resulted in a 38% monthly increase (from 2,844 to 3,930) between July 2004 and December 2004, in the number of cases being created. Despite this increase in the number of cases being added each month, the force has maintained its overall performance, just outside of the target of 90%.

2.5.2.4 Nevertheless, HMIC PNC Compliance Auditors did discover a couple of weaknesses within the process that either result in poor quality data being submitted or an administrative burden for the PNCB. Firstly, when officers complete the PNC1, there is no logical validation within the software, nor is any manual check carried out by supervision in the custody suites. The result is that some officers simply fill in certain fields with full stops in order to bypass the field and speed up the process of completing the PNC1, resulting in poor quality data and the need for PNCB to chase up the officer to complete the information correctly. The second weakness is the current process in which the PNCB update the custody system with the Arrest/Summons number when it has been generated on PNC, this is then followed by the PNCB collating the numbers in a list and faxing the list back to the custody suites. The faxing of the lists causes an additional administrative burden upon PNCB when the data is already available to the custody suites via the custody system.

2.5.2.5 HMIC PNC Compliance Auditors are aware that changes are planned to the custody system to implement a new interface direct to PNC. The project includes the implementation of additional controls within the custody system to improve the quality of data, however, HMIC PNC Compliance Auditors are of the opinion that the need for quality data should be enforced immediately to enable a culture change amongst officers prior to the interface going live.

Recommendation 10

Her Majesty's Inspector of Constabulary recommends that in anticipation of a new interface to PNC, the force impose a more rigid approach to quality control within the custody suites. The force should ensure that the required culture change is initiated to improve data and remove administrative inefficiencies throughout the process of creating Arrest/Summons reports.

2.5.3 Data Quality

2.5.3.1 With regards to data quality, HMIC PNC Compliance Auditors reviewed the quality of data being submitted by officers for input to PNC and also the level of quality that PNCB operators were updating on the PNC.

2.5.3.2 As mentioned in paragraph 2.5.2.4, HMIC PNC Compliance Auditors are concerned with the level of quality of the data being submitted by officers on the PNC1 form. During reality checks conducted by HMIC PNC Compliance Auditors, the poor quality was evident in 48% of the forms checked. Only 15 PNC1 forms were checked, however, with poor quality in such a high ratio of forms and anecdotal evidence from staff within PNCB, HMIC PNC Compliance Auditors are of the opinion that the issue is a forcewide problem that requires attention. The main error identified on the PNC1 forms was incomplete data, however, in some cases, the missing data was integral to the creation of the report on PNC, for example the offence details, therefore, PNCB had to make further investigations before update to PNC could commence. Recommendation 10 of this report should enable the force to improve the quality of information at officer level.

2.5.3.3 In terms of the quality of data being entered to PNC by PNCB staff, HMIC PNC Compliance Auditors found no major problems. HMIC PNC Compliance Auditors found minor problems, confined to typographical errors but they are not considered as an area of concern. Within the PNCB there exists a regime in which a percentage of a PNC operators work is quality assured. The results of the quality assurance is recorded and used in the PDR of the staff. This regime enables the PNC Manager to become aware of any weak areas amongst the staff and develop plans to improve the quality of work. HMIC PNC Compliance Auditors consider the approach to quality assurance as good practice within Sussex Police.

2.5.4 Court Results

2.5.4.1 Over the last 12 months, the force has improved the overall performance in timeliness of court results. The development of an innovative electronic system to deliver court results and remands on a case by case basis to the Sussex Police intranet has played a significant role in this improvement. Whilst the system has provided significant performance improvements, HMIC PNC Compliance Auditors found a number of areas in which the system, if improved, could provide additional efficiency savings for the PNCB.

2.5.4.2 When the information is received from the courts system onto the intranet, the data resides in a 'pending' queue which staff within PNCB review to identify whether the case has been finalised or remanded to a future date. This process is carried out in order to prioritise the court results ahead of the remands and assists the drive towards the performance target. Due to the various skill levels within PNCB, the responsibilities for resulting and updating remands are split between different staff. The combination of the way that the information is delivered to the 'pending' queue and the split responsibilities means that the PNCB suffers from duplication of effort because the intranet system cannot distinguish between results and remands. This means that a person with responsibility for updating results may have to view a number of remand cases before finding a finalised case. The same scenario exists for staff completing remands.

2.5.4.3 In addition, when PNCB have completed the update on PNC, there is a button on the intranet that should be clicked to remove the case from the 'pending' queue, leaving only outstanding updates on the system. The 'click' of this button is wholly dependent on the operator and it is not reviewed as part of the QA procedure by line supervision. In view of this, there is a risk that further duplication can occur if operators are reviewing cases that have already been updated. HMIC PNC Compliance Auditors found an example of this during reality checks of the intranet based system.

2.5.4.4 The force may also be suffering from restrictions allowing them to improve the performance in court resulting because the intranet based system does not indicate whether all results for a particular court on a particular date have been received. The force is reliant upon the courts to send all of the information and are currently operating on an element of trust. However, if the courts do not transfer all cases at the appropriate time, then subsequently deliver them after a long period, this will affect the overall performance attributed to the force. Anecdotal evidence was provided to HMIC PNC Compliance Auditors that this has occurred in the past.

2.5.4.5 The system does provide some management information but is not comprehensive. A performance summary is available at the click of a button, providing immediate results, however, HMIC PNC Compliance Auditors question the limited value that the information provides. For example, all data produced is an 'overall' statistic. The system does not break the performance down by calendar month or by individual courts, therefore, the force cannot identify whether one court is better at providing results than another. This type of information, if available, would be useful to raise at meetings between the force and court managers, as mentioned in recommendation 9, to improve performance of the courts.

Recommendation 11

Her Majesty's Inspector recommends that improvements in the level of management information available from the intranet based system for the receipt of court results be investigated to provide the force with more meaningful data. Improved management information can enable the force to identify potential areas for performance improvements.

2.5.5 Ad-Hoc Intelligence Updates

2.5.5.1 Ad-Hoc intelligence updates are the updates made to PNC that originate from a source other than the creation of report on the PNC. Examples are intelligence submissions by officers that include data applicable to PNC, or the identification of a new address as a result of a stop check on the street.

2.5.5.2 Officers make intelligence submissions to the Source Co-ordinator within the divisional intelligence units (DIU) using a form known as the C22. The source co-ordinator rates the information on the local intelligence system and then if the information is applicable to PNC, the information should be sent to the PNCB for update onto PNC. HMIC PNC Compliance Auditors found inconsistencies in this process because there are varying levels of knowledge amongst DIU staff. Some staff regularly send information to the PNCB but anecdotal evidence was provided from PNCB staff that no information has been received from some DIUs. HMIC PNC Compliance Auditors are of the opinion that in conjunction with recommendation6 of this report, the process for submitting ad-hoc intelligence updates to PNCB should be reinforced amongst DIU staff.

2.5.5.3 Other sources of ad-hoc updates include new information that becomes available from data supplied on a Criminal Records Bureau (CRB) check. The Disclosure Unit within Sussex receives all CRB checks and if any new information comes to light on the check, the information is sent to the PNCB for updating on PNC. Updates from the disclosure unit are more frequent and consistent.

Recommendation 12

Her Majesty's Inspector of Constabulary recommends that the process for submitting intelligence updates to PNCB should be reinforced amongst al Divisional Intelligence Unit staff to ensure that submissions are consistent and relevant to PNC.

2.5.7 The PNC Bureau

2.5.7.1 The PNC Bureau conducts all updates to PNC and also deals with all telephone enquiries from officers and police staff around the force. For the purpose of this report, HMIC PNC Compliance Auditors felt that the enquiry service over the telephone is worthy of note.

2.5.7.2 PNC enquiries are usually made by officers carrying out routine checks whilst on patrol or to gather information during preliminary inquiries from a police station or specialist office. In the case of routine checks whilst on patrol, these checks would normally be conducted over the radio to the resource centre in order to get an immediate response. Checks made from within a police station or specialist office would normally be carried out over a landline telephone or using an officers mobile telephone to the PNCB. Historically, the number of checks carried out over the radio exceeded the number of checks made over the telephone.

2.5.7.3 Sussex Police are in the process of implementing the Airwave radio system across the county. As part of the implementation, the option to include telephony on the Airwave handsets has been incorporated into the project. With this new functionality available to officers, staff in the PNCB reported that they have experienced an initial increase in the number of telephone calls received for routine enquiries. The PNC Manager is monitoring the increase in calls on a monthly basis, however, HMIC PNC Compliance Auditors are concerned that if the number continues to increase, it could have a detrimental effect on the ability of the bureau to maintain current performance on PNC input. The force has a policy that states operational checks whilst on patrol should be conducted via the resource centre, therefore, this policy must be reinforced to reduce the impact on PNCB.

2.5.7.4 In addition to the increase in the number of calls, HMIC PNC Compliance Auditors learned that there is limited structure concerning the receipt of calls. The telephone system works on a 'hunter' basis that operates on the concept of a group of telephone numbers being accessed through one line. If one of the numbers is busy, the system automatically searches for an available number in the group. Whilst this can provide an improved service to staff outside the PNCB, it can disrupt staff in PNCB if they are in the middle of a complex update on the system. To combat this, staff have dual screens, however, HMIC PNC Compliance Auditors are of the opinion that interruption during updates can have an impact on overall efficiency of staff.

2.5.7.5 HMIC PNC Compliance Auditors feel that designated responsibilities amongst staff, for example, staff dedicated to answering queries whilst others are dedicated to updating may improve the efficiency of the PNCB whilst maintaining the level of service to the force.

Recommendation 13

Her Majesty's Inspector of Constabulary recommends that;

- **In order to reduce the impact of increased availability of telephony on the PNC Bureau, the force should reissue and reinforce the policy for contacting the resource centres for operational PNC checks**
- **The PNC Bureau should consider assigning designated responsibilities to reduce the number of interruption to staff making updates and improve efficiency within the bureau.**

2.6 Results

2.6.1 Sussex Police have experience a slight decline in performance over the last twelve months with regards to the creation of Arrest/Summons reports. However, this is due to the decision by the force to enter all cases onto PNC, including records of police bail and those for penalty notices of disorder. The decision led to a monthly increase of 38% in the number of cases being created between July 2004 and December 2004. In January 2004, 88.5% of cases were created within 24 hours rising to a peak of 89% in May 2004. This reduced to 77.8% in September just after the full implementation of the new processes to record all arrests, but has since risen to 80.1% in December 2004. Despite this increase, the force is still performing below the standard required by the new code of practice. In terms of the number of days to enter the best 90% of records, performance has remained consistent over the last twelve months. In January 2004, 90% of cases were taking 7 days to be created on the PNC, this improved to 2 days in May 2004 but the latest statistics available show that in December 2004, performance had slipped slightly to 6 days

2.6.2 A similar tend is also evident in the performance of court resulting. In the first six months of 2004, significant improvements were made in the percentage of cases being updated within the target time of 7 days, following the implementation of the new intranet based system. However, this performance has declined slightly in the final quarter of the year. In January 2004, 12.4% of court results were updated on PNC within 7 days, rising to 59.7% in August 2004. Latest data shows that in December, this figure had reduced slightly to 47.1%. With regards to code of practice, the current performance is below the required standard, however, HMIC PNC Compliance Auditors are aware that an increased number of staff are being trained in order to improve the performance in this area. In terms of the number of days to achieve 90% of cases, performance has also declined overall in the last twelve months. In January 2004, it was taking 56 days to enter the quickest 90% of cases, this figure improved to 20 days in February 2004, but has since declined further to 78 days in December 2004.

2.6.3 The number of Impending Prosecutions has increased from 6,402 in January 2004 to 10,733 in December 2004, an increase of 68%. Part of this increase is attributable to the force commencing the update of all cases on PNC at the commencement of proceedings, nevertheless, HMIC PNC Compliance Auditors would expect the overall number to level out and start to decrease again with effective management of the cases. A process already exists in which a list is sent to each Criminal Justice Department to review old cases, however, in order limit the increase in the total number of cases, the force must ensure that the process is carried out regularly. In addition, in order to satisfy itself that the numbers are being managed, the overall number of cases should be monitored on a monthly basis.

2.6.4 A graph illustrating these performance figures can be seen in Section 1 of this Report at paragraph 1.4.11.

Appendix A

A Summary of Good Practice within Sussex Police

- Data Protection and IT Security training is provided to new staff and during IT related training courses. Candidates are also required to sign a statement declaring their awareness of their own responsibilities.

- The provision of PNC Training is linked to staff PDRs to ensure that training is only delivered where there is a genuine need.

- Post training evaluation is carried out by the training department who contact the line manager of trainees two weeks after the course has ended.

- The PNC Bureau conducts quality control of the input made within the unit. In addtion, the results of the quality control are recorded and used within staff PDRs.

Summary of Recommendations for Sussex Police

Recommendation 1

Her Majesty's Inspector recommends that in order to improve the level of management information available to BCU Commanders and custody managers, thus increasing accountability of officers, consideration should be given to upgrading the reporting function of the 'Errors Database'.

(Paragraph 2.1.5)

Recommendation 2

Her Majesty's Inspector of Constabulary recommends that the force develop a strategy for PNC in order to meet the short, medium and long-term demands of the system. Any strategy should include provision for future developments to the system, procedural impacts and marketing of changes to all relevant personnel.

(Paragraph 2.2.2.3)

Recommendation 3

Her Majesty's Inspector of Constabulary recommends that the force continue with its plans to develop a PNC policy, consolidating and updating all existing policies. The development and publication of the policy will ensure that all staff either using or updating PNC data are aware of their responsibilities.

(Paragraph 2.2.3.3)

Recommendation 4

Her Majesty's Inspector of Constabulary recommends that the force urgently reviews the administration process surrounding the access control to PNC via Mobile Data Terminals. System administrators should be in receipt of an authorisation prior to granting access to new users. In addition, the force should reinforce the Information Security Policy concerning the control of passwords on IT systems.

(Paragraph 2.2.4.6)

Recommendation 5

Her Majesty's Inspector of Constabulary recommends that;

- the force considers the level of resources assigned to the Access to Information Team to ensure that a sufficient assurance can be gained from the activities conducted by the team.
- in order to comply with the code of practice for PNC and to gain assurance concerning the data that is being processed within force, the force should urgently consider the development of a risk based audit plan covering all IT systems.
- the force should also ensure that PNC related matters resulting from Data Protection Audits are 'owned' by the Intelligence Steering Group to ensure an effective follow up.
- The force retains the process for transaction monitoring within the Access to Information team and increases the number of transaction monitoring checks conducted on a regular basis.

(Paragraph 2.2.5.6)

Recommendation 6

Her Majesty's Inspector of Constabulary recommends that as part of the development of a PNC Strategy (see Recommendation 2), the force develops a marketing strategy to raise awareness of PNC functionality amongst all staff.

(Paragraph 2.3.1.6)

Recommendation 7

Her Majesty's Inspector of Constabulary recommends that in light of the secondment of PNC trainers to long term projects, the force consider its position concerning the delivery and availability of PNC training.

(Paragraph 2.3.2.5)

Recommendation 8

Her Majesty's Inspector of Constabulary recommends that the force urgently considers the quality and delivery of training for PNC access via Mobile Data Terminals. The training should be of a measurable standard and where possible, comply with national standards.

(Paragraph 2.3.2.9)

Recommendation 9

Her Majesty's Inspector of Constabulary recommends that the force reintroduce the meetings between Criminal Justice staff and the Magistrates Courts. The meetings should also involve a representative from the PNCB management team to ensure that issue affecting performance can be raised pursued.

(Paragraph 2.4.1)

Recommendation 10

Her Majesty's Inspector of Constabulary recommends that in anticipation of a new interface to PNC, the force impose a more rigid approach to quality control within the custody suites. The force should ensure that the required culture change is initiated to improve data and remove administrative inefficiencies throughout the process of creating Arrest/Summons reports.

(Paragraph 2.5.2.5)

Recommendation 11

Her Majesty's Inspector recommends that improvements in the level of management information available from the intranet based system for the receipt of court results be investigated to provide the force with more meaningful data. Improved management information can enable the force to identify potential areas for performance improvements.

(Paragraph 2.5.4.5)

Recommendation 12

Her Majesty's Inspector of Constabulary recommends that the process for submitting intelligence updates to PNCB should be reinforced amongst al Divisional Intelligence Unit staff to ensure that submissions are consistent and relevant to PNC.

(Paragraph 2.5.5.3)

Recommendation 13

Her Majesty's Inspector of Constabulary recommends that;

- In order to reduce the impact of increased availability of telephony on the PNC Bureau, the force should reissue and reinforce the policy for contacting the resource centres for operational PNC checks
- The PNC Bureau should consider assigning designated responsibilities to reduce the number of interruption to staff making updates and improve efficiency within the bureau.

(Paragraph 2.5.7.5)

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.