



DEVON and CORNWALL CONSTABULARY

3 - 7 JULY 2006

**POLICE NATIONAL COMPUTER
COMPLIANCE REPORT**

Table of Contents

1. Executive Summary	1
1.1 Introduction	1
1.2 Background.....	1
1.3 Methodology	2
1.4 Current Performance.....	3
1.5 Conclusions	4
2. Detailed Findings and Recommendations	6
2.1 Leadership	6
2.1.1 PNC Steering Group	6
2.1.2 Responsibility and Accountability	6
2.2 Policy & Strategy.....	7
2.2.1 PNC Policy and Strategy.....	7
2.2.2 PNC Security	8
2.3 People.....	12
2.3.1 Marketing and Awareness.....	12
2.3.2 PNC Training	14
2.4 Partnerships and Resources	16
2.4.1 Relationship with the courts	16
2.4.2 Relationship with non police prosecuting agencies (NPPAs).....	16
2.5 Processes	17
2.5.1 Creation and update of Arrest/ Summons (A/S) reports	17
2.5.2 Update of court information	19
2.5.3 Originator Line	19
2.5.4 Ad hoc intelligence updates	20
2.5.5 Data Quality	20
2.5.6 Impending Prosecutions.....	21
2.6 Results.....	21
APPENDIX A.....	23
SUMMARY OF RECOMMENDATIONS FOR DEVON and CORNWALL	23
APPENDIX B.....	25
SUMMARY OF GOOD PRACTICES AT DEVON and CORNWALL	25
APPENDIX C – ‘ON THE RECORD’	26
APPENDIX D – PRG REPORT	28
APPENDIX E – 1 ST PNC REPORT.....	30
APPENDIX F – 2 ND PNC REPORT.....	32

1. Executive Summary

1.1 Introduction

- 1.1.1 Her Majesty's Inspectorate of Constabulary (HMIC) conducted a Police National Computer (PNC) Compliance Inspection of Devon and Cornwall Constabulary between 3rd and 7th July 2006.
- 1.1.2 The Constabulary was subject to a PNC Compliance Audit using the July 2005 Protocols on PNC Compliance. Her Majesty's Inspector would like to acknowledge the enthusiasm of the Force and also to place on record her thanks to all members of staff who contributed to this report and provided assistance during the inspection.
- 1.1.3 This report is based on views and comments obtained from strategic, PNC and customer level management and users at Force Headquarters and at 2 of the 4 Basic Command Units (BCU). These views have been supported by reality checks conducted by HMIC PNC Compliance Auditors (hereafter referred to as HMIC Auditors).

1.2 Background

- 1.2.1 Devon and Cornwall Constabulary covers an area of approximately 4,000 square miles and in geographical terms, is the largest territorial police force in England. The force area also includes approximately 550 miles of peninsula coastline and over 13,000 miles of road network, including the M5 motorway. The combination of the vast rural expanses, such as Dartmoor, Exmoor and Bodmin Moor and pockets of densely populated areas in Plymouth, Exeter, Torbay and Truro, in conjunction with the road infrastructure and geographic properties, provides the force with a variety of policing challenges. The resident population of the force area is 1.6 million, however, this figure increases by almost 12 million with the number of visitors and tourists during the year. There is also an international airport in Exeter, a number of domestic airports within the county and large ferry port at Plymouth.
- 1.2.2 The Force headquarters is located in Exeter and policing activity is provided from four BCUs, namely Cornwall and the Isles of Scilly, Plymouth, North and East Devon and South and West Devon.
- 1.2.3 The Force is headed by the Command Team which consists of the Chief Constable, Deputy Chief Constable (DCC), three Assistant Chief Constables (ACCs) with individual responsibilities for Operations, Operational Support and Territorial Policing and Partnership. There is also a Director of Finance and Administration. The Constabulary employs¹ 3,462 full-time equivalent police officers, 2,165 police staff, 562 Special Constables and 75 Police Community Support Officers.
- 1.2.4 The management of the PNC sits within the portfolio of the ACC with responsibility for Operations. At micro level, the PNC is managed within Force Intelligence in the management structure of the Crime Department.

¹ Data accurate as of 31st January 2006

- 1.2.5 The creation of Arrest/ Summons records at Devon and Cornwall is a semi-automated process with officers completing a record on the force Criminal Intelligence System (CIS). The CIS record is then placed in a queue within the system where it is quality assured by staff in the Force National Computer Bureau (FNCB). Once the quality assurance process is complete, FNCB staff initiate the electronic transfer of the record to the PNC via the force interface. The force does not use skeleton records as a full record is available from CIS. Staff in FNCB are also responsible for monitoring the interface to ensure that all transmissions are successful and that any failures do not impact on performance.
- 1.2.6 The FNCB also provides a 24/7 service for making operational updates to the PNC on behalf of the force. These include Wanted/Missing reports, Stolen Vehicles and Disqualified Driver updates. The FNCB also provides telephone checks and specialist advice for officers, and performs enhanced searches on the system, such as Vehicles On Line Descriptive Searches (VODS) and Queries Using Extended Search Techniques (QUEST).
- 1.2.7 Magistrate court results are received directly from the courts into the three Records and Convictions Units. These are situated at Camborne, Plymouth and Exeter. Staff update the results on CIS and the result is automatically transferred to PNC. In some instances, cases will not transfer over the interface, therefore, some manual input to PNC is required. The force updates all information from the court registers including disposals, remand histories and bail conditions. The receipt of crown court results varies depending on the area. Camborne have commenced the use of the Xhibit system, whilst Plymouth and Exeter rely on the use of a courier system to receive hard copies of the results from crown court hearings.

1.3 Methodology

- 1.3.1 A full inspection against the 2005 PNC Protocols was carried out, covering the sections of Leadership, Policy and Strategy, People, Partnerships and Resources, Processes and Results.
- 1.3.2 The inspection was conducted over three stages with a final assessment being provided in line with the current HMIC Baseline Assessment grading structure of:
- **Excellent** – Comprehensive evidence of effective activity against all protocol areas.
 - **Good** – Evidence of effective activity in many areas, but not comprehensive.
 - **Fair** – Evidence of effective activity covering some areas, but concerns in others.
 - **Poor** – No or limited evidence of effective activity against the protocol areas, or serious concerns in one or more area of activity.

1.3.3 The first stage of the inspection involved the force providing HMIC Auditors with documentation to support its adherence to the protocols. This was followed up by a visit to the Force with HMIC Auditors conducting numerous interviews with key staff. The visit to the Force also incorporated the final stage of the inspection, which was based upon reality checks. The reality checks included reviewing PNC data against source documents and a review of PNC policy documentation.

1.3.4 Using the evidence gathered during each stage of the inspection, this report has been produced based upon the European Foundation of Quality Management (EFQM) format.

1.4 Current Performance

1.4.1 On 27th April 2000, ACPO Council endorsed the ACPO PNC Compliance Strategy. The strategy is based upon the following four aspects of data handling:

- Accuracy
- Timeliness
- Completeness
- Relevancy

1.4.2 The strategy is owned by ACPO but is also reliant on other partners taking responsibility for key actions within the strategy. The partners include Centrex, HMIC, Police Information Technology Organisation (PITO) and individual forces.

1.4.3 On 1st January 2005, the performance indicators of the ACPO Compliance Strategy were replaced by the timeliness standards contained within the newly published Code of Practice for the PNC. The PNC Code of Practice, developed by the National Centre for Policing Excellence and endorsed by ACPO, is a statutory code made under s.39a of the Police Act 1996 (inserted by section 2 of the Police Reform Act 2002). It provides scope for the Home Secretary to invoke statutory intervention for forces failing to comply. With regards to individual forces, a number of performance indicators (PIs) specifically for PNC data standards were set. Each force has a responsibility to achieve the standards set within the Code of Practice. The timeliness standards within the Code are as follows:

- 90% of recordable offences entered onto PNC within 24 hours of the commencement of proceedings. The commencement of proceedings being defined as when a person is arrested, reported or summonsed.
- 50% of all finalisations being entered onto PNC within 7 days of the information being received by the police. This target increased to 75% on 1 July 2005, six months after the commencement of the

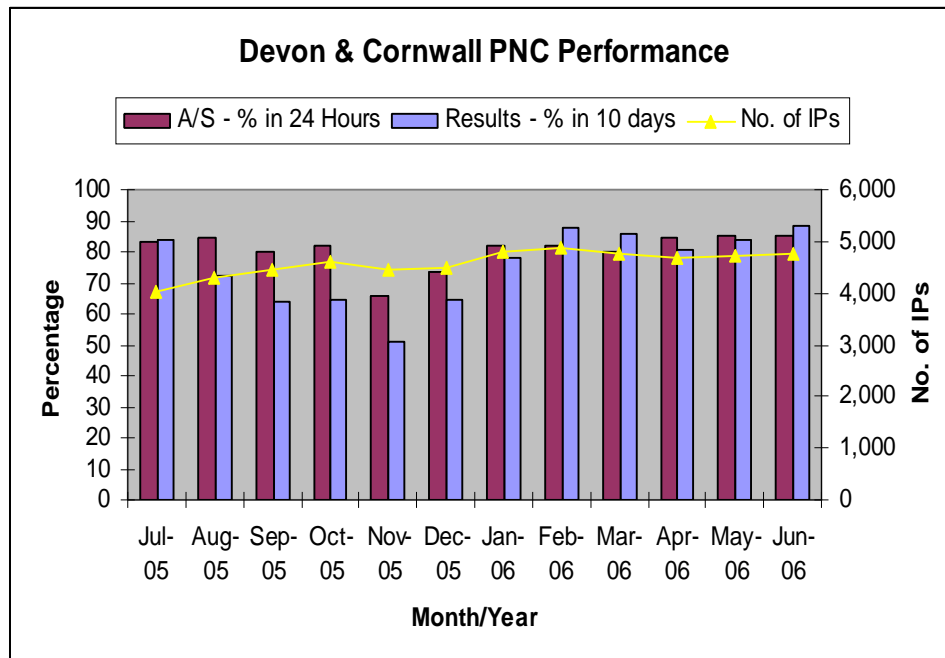
Code. (Courts have their own target of 3 days for delivery of data to the police. Therefore, the police are measured against an overall target of 10 days.)

1.4.4 In June 2006, Devon and Cornwall Constabulary input 85% of Arrest/Summons (A/S) updates onto the PNC within 24 hours. This shows a slight improvement in performance in the 12 months from June 2005 when 81.9% of cases were input within 24hours. Current performance is below the national average for England and Wales of 86.1%.

1.4.5 In terms of disposals, the force has consistently achieved the target of 75% within 10 days for each of the last six months. In June 2006, 88.4% of cases were input within 10 days, the highest the force has recorded in the last twelve months. Over the last twelve months, performance has ranged from 50.7% to 88.4% with the target being achieved in 7 of the last twelve months.

1.4.6 With regards to Impending Prosecutions (IPs) on the PNC, in the 12 months to March 2006 the Force has shown an overall increase of 23%. In April 2001, HMIC supported by the Home Secretary stated that all forces should be in a position to confirm that any outstanding case that is over twelve months old, is legitimately outstanding. In Devon and Cornwall, this accounts for only 7.2% of all their outstanding prosecutions and is within the profile established by HMIC in 2001.

1.4.7 A graph illustrating Devon and Cornwall's performance in the 12 months to March 2006 is shown below:



1.5 Conclusions

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

Good – Evidence of average/above average performance against the ACPO performance indicators and effective activity covering many areas, but not comprehensive.

- The Force inputs a full record onto the PNC as soon as the Arrest Summons report is created.
- All court adjournments and remands are entered onto the PNC along with police and court bail with and without conditions.
- All PNDs (Police Notices for Disorder) and all arrests under section 9 and 10 of the Criminal Justice Act are recorded on PNC
- There are concerns regarding the lack of a formal assessment at the end of PNC courses delivered by the Sunguard Vivista trainers.
- The practice of giving the Force National Computer Bureau and the Records and Convictions staff their own PNC access prior to a PNC course is against a previous PNC thematic recommendation.
- The Arrest Summons report input is still below the ACPO PNC Code of Practice target.

1.5.2 A summary of good practice points, along with recommendations for improvement can be seen in Appendix A and B of this report.

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

- Police Research Group Report – ‘Phoenix Data Quality’, *published 1998*
- HMIC Thematic Inspection Report – ‘On The Record’, *published 2000*
- HMIC Report – ‘PNC Data Quality and Timeliness, 1st Report’, *published 2001*
- HMIC Report – ‘PNC Data Quality and Timeliness, 2nd Report’, *published 2002*

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

2. Detailed Findings and Recommendations

2.1 Leadership

2.1.1 PNC Steering Group

2.1.1.1 At the time of inspection, Devon and Cornwall Constabulary had a well established PNC Steering Group (PSG). HMIC auditors were provided with evidence that each meeting of the group is chaired by a chief officer and that the membership of the group includes all relevant staff who can have an impact and drive change in relation to the PNC. In addition, the agenda items for the meetings are such that the force is able to tackle key issues when they arise. For example, during the most recent meeting in April 2006, an item was included to discuss ways of increasing the level of investigative use that is made of the PNC in order to gain most benefit from the system.

2.1.1.2 HMIC Auditors were also pleased to see evidence of documented terms of reference for the PNC Steering Group. The terms of reference outlines the required membership of the group and also takes account of the areas of activity within the force that have an impact on the PNC in addition to taking cognizance of previous thematic reports relating to the PNC and ACPO publications on Information Management. However, despite the comprehensive references to previous publications within the terms of reference, HMIC Auditors were disappointed that compliance with the Code of Practice for PNC was not included.

2.1.1.3 One other area for improvement that was identified in relation to the PNC Steering Group was the frequency and timing of meetings. In order to gain most benefit from the meeting, the force should consider aligning the meeting to coincide with the period when Regional and National Meetings are taking place (The South West Regional PNC Liaison Officer Conference and P4G²), usually on a quarterly basis. This will enable the group to remain fully apprised of regional and national issues that could affect the use and management of the PNC within the force.

Recommendation 1

Her Majesty's Inspector of Constabulary recommends that the terms of references for the group be updated to include the statutory code of practice for PNC. The group should also consider timings the meetings to align with regional/national groups.

2.1.2 Responsibility and Accountability

2.1.2.1 The PNC Bureau collates a range of statistics pertaining to the quality and timeliness of source input documents (SIDs) submitted by each

² P4G – Police PNC Policy and Prioritisation Group, a National Strategic Group chaired by an ACPO Officer who holds the portfolio for the PNC.

BCU. The statistics break down the performance by BCU to enable easy identification of any poor performing areas, furthermore, the statistics show the origin of the record, e.g. charge, caution, Fixed Penalty Notice, to provide further opportunity to examine local process to identify the cause if there is a failure to submit documents or documents are submitted late. In addition, there is information relating to any SID that is returned to the BCU because of poor quality or insufficient data contained in the document. This data is also broken down by BCU and breaks down the total by the types of error being made. HMIC Auditors consider the production of statistics in this way to be good practice.

2.1.2.2 When the statistics are produced, the files are placed on a corporate drive on the force network to enable BCU and Departmental Commanders to freely view them. This provides suitable access to all senior managers on the BCU and in the Departments to view the data.

2.1.2.3 In addition to the production of data to hold police officers and detention officers to account, HMIC Auditors also reviewed the level of accountability placed upon BCU and Departmental commanders by Chief Officers. Within the force, there are no longer Performance Review Inspections carried out by Chief Officers. These were replaced by self-assessment inspections in which the BCU or department identifies any risks or areas in need of improved performance. The self assessment process is then used to inform chief officers of what action is being taken.

2.1.2.4 During the course of the inspection, HMIC Auditors discovered that performance against PNC targets does not form part of the self-assessment process on the BCUs. With the change of responsibility for updating SIDs being transferred to the Detention Officers and subsequently, the Criminal Justice Department (CJD), HMIC Auditors are of the opinion that due to the impact that CJD can have on overall PNC performance, the force should ensure that self-assessment of CJD should include a standing item on PNC performance.

Recommendation 2

Her Majesty's Inspector of Constabulary recommends that the Force ensures that PNC Performance is considered as a standing item in the self-assessment process of the Criminal Justice Department.

2.2 Policy & Strategy

2.2.1 PNC Policy and Strategy

2.2.1.1 HMIC Auditors were pleased to note the existence of a comprehensive PNC policy in Devon and Cornwall Constabulary. The policy is stored electronically and can be accessed by all staff at any time. In addition, the database where the policy is stored also includes a facility which records the date that a policy was last revised. This date is then used to prompt the BCU or department which owns the policy to review the

policy on a regular basis. In the case of the PNC policy, the review is carried out annually. This is considered to be good practice by HMIC Auditors.

2.2.1.2 With regards to a PNC Strategy, the Force has also produced a documented PNC Strategy. The strategic aims of the force regarding the use of the PNC are outlined in the strategy as well as a comprehensive list of objectives that the Force has in order to meet these aims.

2.2.1.3 However, an area for improvement identified by HMIC Auditors is the development of a strategic action plan that can be used to support the objectives. Whilst the documented objectives state what the force wants to achieve, there is currently no evidence of how the force will deliver the objectives. An action plan will enable the force to develop specific actions, assigned to individual members of staff within the force with target dates for completion and provide an ability to track progress under the auspices of the PNC Steering Group. The action plan should also be maintained as a dynamic document, adding new actions when they arise, for example, as a result of recommendations made in this report of data protection audit reports carried out by the force. The management of a strategic plan will ensure that the force maintains its position of being proactive with regards to the PNC.

Recommendation 3

Her Majesty's Inspector of Constabulary recommends that the Force develop a strategic action plan to support the delivery of the aims and objectives contained within the PNC Strategy. The action should be dynamic to reflect the changing face of the PNC and be owned and managed by the PNC Steering Group.

2.2.2 PNC Security

2.2.2.1 With regard to system security, HMIC Auditors reviewed five key areas. These are User Access, Transaction Monitoring, Data Protection Auditing, the Role of Professional Standards and Information Security/ Data Protection Training. Some good practices and some areas for improvement were identified during the review and these are discussed further below.

2.2.2.2 Access to the PNC is gained via an interface on the force's Operational Intelligence System (OIS) or through a Criminal Justice Exchange (CJX) gateway using a web browser. Users are set up separately depending on they are going to access the PNC.

2.2.2.3 Users who access PNC via the OIS interface are set up by the system administrators who provide IT support for the force. The system administrators monitor the attendance records for PNC courses and update the user access on OIS accordingly. There is no formal communication between the trainers and the system administrators.

The level of access is determined by the role of the person who has attended the training course.

- 2.2.2.4 Access via the CJX is provided upon application by a member of staff who has already received access via the OIS interface. The PNC Bureau manages access via the CJX due to the limited number of User IDs that are available.
- 2.2.2.5 With regards to the maintenance of the user groups, the CJX groups are monitored on a monthly basis to ensure that all users IDs are currently active on the system. If a user ID is not being used, the person using the ID loses the privilege and the user ID is allocated to somebody else. This process does not affect any access to PNC via the OIS interface.
- 2.2.2.6 For staff who access the PNC via the OIS interface, their access is only removed if they leave the force, are subject to a long term absence or are subject to disciplinary proceedings which requires their access to be suspended. Human Resources notify the system administrators on a regular basis of any staff who fall into the above categories. HMIC Auditors are satisfied that the removal in these instances is being managed effectively. However, there is some concern regarding the levels of access of staff who change within the force. Currently, there is no process, or policy regarding the levels of access for staff who change roles within the force. The current philosophy is that once a user is trained on PNC, they retain access to the system regardless of the role they carry out.
- 2.2.2.7 It is the opinion of HMIC Auditors that in order to maintain a high level of security on the system, only users who access PNC as part of their core role should have access to the system. Therefore, if for example a user in a control room who could have a high level of access, changes jobs to work in the finance department, PNC access should be removed. This will ensure that the Force increases the level of control on who is accessing the PNC and also ensuring increasing the likelihood that all transactions are carried out for a legitimate policing purpose.
- 2.2.2.8 The Force should consider introducing a policy and process whereby access is only provided to staff who need it as part of their role. In addition, whilst HMIC Auditors do not question the integrity of the staff involved in the administration of user access, there is some risk to the organisation in having individuals able to make such changes to system access with no independent auditing of the activity being carried out. An audit of the current list of User IDs will also enable the force to identify and remove users from the system who no longer require that access for their current role.

Recommendation 4

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

- **Introduces a policy and process to ensure that only staff who require PNC access as part of their role are provided with access to the system;**
- **Introduces an independent audit, at least annually, of all user access administration**

2.2.2.9 Transaction monitoring is a requirement of the ACPO Data Protection Audit Manual. It is a process where police officers and staff are asked to verify their reasons for performing transactions on the PNC and, as such, is an important activity in the prevention and detection of misuse or abuse of the PNC. At Devon and Cornwall this is a function that is carried out by staff in the Data Protection Unit.

2.2.2.10 Staff in the Data Protection Unit select transactions at random on a daily basis and send the information via an Unsolicited Message (UM) on the force OIS system to the user who carried out the check. The individual who requested the check is asked to confirm that it was conducted for operational policing purposes by printing off the UM, appending the reasons for the check to the printed form and having the form endorsed by their line manager. The form should then be returned to the Data Protection Unit for collation of responses. Using this method the Data Protection Unit is able to monitor the returns to ensure that all transaction monitoring requests are accounted for.

2.2.2.11 HMIC Auditors view the process as good practice because it provides the force with an efficient process and also ensures checks are verified as soon as practicable after the PNC transaction has been carried out. However, there is some concern regarding the involvement of line managers in the process. During interviews and focus groups, HMIC auditors were provided with anecdotal evidence that some line managers do not verify the reasons for the PNC transaction being explained by their subordinates. Some line managers take the reason at face value and sign the form as verified without having checked the source of the transaction. This approach can undermine the whole process and therefore, the Force needs to ensure that line managers are held accountable for their verification. HMIC auditors are of the opinion that by endorsing the transaction monitoring form, line managers are verifying that PNC transactions are carried out for a legitimate policing purpose. This level of accountability should be included the PNC policy and should also be supported by dip sampling of the returned forms by the Data Protection Unit.

Recommendation 5

Her Majesty's Inspector of Constabulary recommends that the Data Protection Unit commence a process of dip sampling returns from line managers in respect of transaction monitoring.

- 2.2.2.12 Data Protection Audits are planned on a yearly basis by the Data Protection Officer (DPO). The DPO performs a risk assessment of its IT data systems following which, decisions are made as to which systems are audited. With regards to the PNC, the PNC Manager is involved in the risk assessment to ensure that the DPO is fully apprised of the system. This process complies with the ACPO Data Protection and Audit Manual.
- 2.2.2.13 When audits are conducted, the reports contain recommendations to improve business processes where it is found that the process has contributed to inefficiencies or errors in the data. The reports also include classification of errors that are also in accordance with the ACPO Data Protection and Audit Manual. Upon completion of the audit when the report is published, it becomes the responsibility of the PNC Steering Group. In addition, any recommendations that are made in the reports are entered onto a Continuous Improvement Database. The database is managed by Corporate Development who ensures effective follow up of the recommendations. HMIC Auditors are also of the opinion that any recommendations should form part of a strategic action plan for the PNC. (See Paragraph 2.2.1.3)
- 2.2.2.14 HMIC Auditors also reviewed the role of the Professional Standards Department with regard to PNC issues within Devon and Cornwall. Professional Standards are independent of operational activities and has its own PNC trained operators to provide a research capability, such independence is viewed as good practice. However, when the use of staff with expert knowledge is required, PSD utilise staff from within the force under the terms of a confidentiality contract. The confidentiality contract is used as a control to reduce the risk of information relating to sensitive investigations being leaked throughout the Force. HMIC Auditors consider this to be good practice, however, they are also of the opinion that the need for the contract could be removed if staff within Professional Standards were given additional training and delegated as 'authorised signatories'³ with Hendon Data Centre.
- 2.2.2.15 In addition, there are strong links between the Data Protection Officer and Professional Standards in order that Professional Standards are alerted to any suspicions regarding the use of the PNC. One area for improvement identified by HMIC Auditors is that the PSD only reacts to allegations and does not perform any proactive monitoring of PNC

³ Hendon Data Centre hold a list of staff who are authorised to request historical data from the PNC in order to assist in criminal or internal investigations.

transactions to enable potential misuse or abuse to be identified. It is therefore possible that the Force may be missing opportunities to detect system abuse and misuse.

Recommendation 6

Her Majesty's Inspector of Constabulary recommends that the Force consider options for the proactive monitoring of PNC activity.

- 2.2.2.16 Finally with regard to PNC system security, HMIC Auditors reviewed the role of the Information Manager (IM) and Data Protection Officer (DPO) with regard to training. At present, the only training provided in respect of training on DP and IM issues is delivered as part of I.T training courses. There is regular communication between the DPO/IM and the IT trainers to ensure that the content of the training is relevant and up to date.
- 2.2.2.17 Whilst HMIC Auditors view the approach to IT training courses as good practice, the lack of any other training means that there are large knowledge gaps surrounding DP/IM issues around the force. HMIC Auditors were informed that induction courses for new staff do not include DP/IM awareness. Furthermore, despite a Computer Based Training package being developed with a mandate that all staff should complete the package, at the time of the inspection, less than 15% of staff had completed it. In other forces, HMIC Auditors have found good practice whereby all staff are mandated to complete training packages regarding Information Security/Management and the completion of the training package is linked to staff appraisal systems.
- 2.2.2.18 HMIC Auditors are of the opinion that with the recent inception of Freedom of Information and the Government Protective Marking Scheme, the force should examine ways of raising awareness of each of these composite parts of Information Management. The review should cover efficient processes to raise awareness amongst all staff.

Recommendation 7

Her Majesty's Inspector of Constabulary recommends that the Force should examine ways of improving the levels of awareness of each aspect of Information Management amongst all staff. Consideration should be given to ensuring that the current mandate is adhered to in order that the current response rate of 15% is improved.

2.3 People

2.3.1 Marketing and Awareness

- 2.3.1.1 The force PNC strategy includes an objective which states that; *"The force will ensure that all staff and their supervisors who are involved in the prevention, reduction and investigation of crime are fully conversant with the PNC research facilities available, to support these relevant*

activities", however, as explained in paragraph 2.2.1.3, there are no specific actions that have been identified to meet this objective. HMIC Auditors are of the opinion that the lack of specific actions has contributed to the varying level of awareness found amongst staff during the inspection.

- 2.3.1.2 The level of awareness amongst staff in the Crime Department was generally higher than for uniformed staff. During interviews and focus groups, staff from the crime department demonstrated a good understanding of the system and were aware of the investigative functionality within the system, for example, VODS⁴ and QUEST⁵. HMIC auditors were also provided with verbal examples of when the system had been put to good use.
- 2.3.1.3 With regards to uniformed staff, there was a stark contrast in the level of awareness that was being demonstrated. In some cases, officers had not heard of the investigative capabilities of the system and had therefore, not used them as part of their duties. HMIC Auditors were disappointed to discover this because they are aware that the Force has made efforts to raise awareness amongst all staff. For example, mock up table menus had been placed in canteens outlining the data that is held on the PNC and various functions that exist to use and research the data.
- 2.3.1.4 During interviews and focus groups, staff were asked how they are kept informed of changes to PNC in order that they are kept up to date with the functionality and any changes in policy. Staff reported that e-mail is the primary media used to communicate changes within the Force, however, operational police officers stated that they do not always have time to read the information in depth. As a result, much of the information is not absorbed properly by staff.
- 2.3.1.5 HMIC Auditors are aware that the force uses PITO to deliver presentations on a regular basis, therefore, they are of the opinion that in order to meet the objective of the PNC Strategy, the force should consider uniformed staff as a target audience when planning future presentations. The force should also continue to develop alternative methods of communicating changes and consider utilising the resources of internal marketing experts within the Corporate Communications Department in order that the benefits of any marketing are maximised.
- 2.3.1.6 One further area of concern that was identified by HMIC auditors was regarding the level of knowledge of ViSOR⁶. The system includes an interface to PNC in order that ViSOR can generate a marker onto the PNC. It is important that staff involved in the policing of violent and sex offenders are aware of the system and the requirements to ensure that data on both systems is up to date. It was therefore of some concern that Neighbourhood Beat Managers who are responsible for carrying out address checks on registered sex offenders, were unaware of

⁴ Vehicle On-line Descriptive Search

⁵ Queries Using Extended Search Techniques

⁶ Violent and Sex Offenders Register

ViSOR. In addition, HMIC Auditors also found a low level of knowledge amongst other operational staff. Without the knowledge of the system, the force may be missing opportunities to record intelligence on offenders who have records on the ViSOR database.

Recommendation 8

Her Majesty's Inspector of Constabulary recommends that the Force develop a programme of awareness presentations targeted at uniformed staff and supervision. The force should also consider the use of internal marketing experts to exploit further opportunities to raise the levels of awareness amongst staff of both PNC and ViSOR.

2.3.2 PNC Training

2.3.2.1 PNC training was an area at Devon and Cornwall in which HMIC Auditors experienced mixed findings with some good practice being identified as well as areas of concern.

2.3.2.2 The Force has the use of three accredited trainers provided by Sungard Vivista, a company to which PNC training has been outsourced. The trainers are only accredited to deliver enquiry level courses. Any update training that is required by the force is provided by either Centrex at Leicester, or the use of another third party accredited company.

2.3.2.3 HMIC Auditors found no concerns with the planning or delivery of the training that is being provided by Sungard Vivista. During interviews and focus groups, staff reported very few delays in obtaining a training course once they had submitted an application. When a member of staff requires a PNC course, an application is made to a training co-ordinator on the BCU. If the training co-ordinator agrees that training is required, the timing and the location of the course is negotiated with the trainers. Due to the geographical size of the force area, the trainers are not confined to delivering PNC courses on one site. Courses can be delivered at a number of locations throughout the force.

2.3.2.4 Whilst HMIC Auditors were encouraged by the way that training is planned, an area for improvement was identified with regards to the assessment of students at the end of the course. All PNC Training must be delivered in line with PICTTS⁷ Occupational Training Standards. PNC Trainers must adhere to these standards in order to retain their accreditation to deliver PNC courses. Part of these standards is the requirement to ensure that all students are subject to a formal, evidence based assessment at the end of the course. However, during the course of the inspection, HMIC Auditors discovered that the training being provided in Devon and Cornwall is not subject to formal assessment. The PNC trainers assess students on an ad-hoc basis throughout the course then form an opinion at the end of the course whether a student should be granted access to the system.

2.3.2.5 In addition to the lack of assessment, HMIC auditors also discovered

⁷ Police Information Communications Technology Training Services

that in the PNC Bureau and the Records and Convictions Units, where staff require 'update' training, new staff are granted access to the system without having attended a formal training course provided by an accredited trainer. Initially, new staff receive their training 'on the job' with the support of a mentor and their supervision, prior to attending a PNC course delivered by an accredited trainer. In 2000 when the thematic inspection report 'On the Record' was published, it stated;

*"It is a requirement of the code under which forces are connected to PNC that all persons having access to PNC must have received the correct training. It has also been agreed, by the PNC Director, NPT and user groups, that training will only be delivered by trainers who have successfully attended the nationally accredited PNC Trainers Course."*⁸

It is therefore of concern that this practice remains to be adopted within the force. The practice should cease immediately and the force must examine alternative arrangements for the delivery of PNC update training.

- 2.3.2.6 A further point to be made in respect of PNC training is with regard to post training evaluation. Evaluation currently takes the form of a "Happy Sheet" which is completed at the end of the course by each delegate. However, the Happy Sheet is primarily for the use by the trainer to ensure that the expectations are being met by the trainees. In the case of Devon and Cornwall where training is outsourced, the benefits of the Happy Sheet are only being realised by Sunguard Vivista who retain all of the feedback. The force must therefore consider the use of post training evaluation to ensure that the training is not only meeting the objectives of the course but also that it is providing value for money by ensuring that trainees are returning to the work place with the necessary skills.
- 2.3.2.7 Post training evaluation should be carried out once a trainee has returned to the workplace and had chance to use the new skills. Only then can the value of the training be assessed. If the volume of trainees is high, the force should consider carrying out the evaluation on a dip sample basis. HMIC PNC Compliance Auditors view the implementation of such an evaluation process to be good practice as it assists in improving training design and delivery.
- 2.3.2.8 Finally with regards to training, HMIC auditors found good practice with regards to new officers joining the force. Student constables on the Initial Police Learning and Development Programme (IPLDP) receive three days of awareness training by one of the accredited trainers from Sunguard Vivista. This awareness is also supported by a presentation delivered by staff from PITO Customer Services.

⁸ 'On The Record – Thematic Inspection Report on Police Crime Recording, the Police National Computer and Phoenix Intelligence System Data Quality' P.115, Paragraph 7.5.2

Recommendation 9

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

- **Immediately cease the training of FNCB and Records and Convictions staff by non-accredited trainers;**
- **Introduce formal assessment processes on all PNC courses, ensuring that they are evidence based and comply with PICTTS Occupational Training Standards;**
- **Consider the benefits of enhancing the training evaluation for PNC courses by introducing post-training evaluation.**

2.4 Partnerships and Resources**2.4.1 Relationship with the courts**

2.4.1.1 The Force has experienced mixed relationships with the courts that service the Devon and Cornwall area. The delivery of court results from the courts to the police is an automated process via a computer link in each Records and Convictions Unit (R&C). However, when there is a need to contact the courts, for example, with queries arising from the court registers, some courts are more helpful than others.

2.4.1.2 When issues cannot be resolved with the courts, a Chief Inspector from the Criminal Justice Department can raise the matter at the Local Criminal Justice Board. However, despite this mechanism being in place, R&C staff reported that inconsistencies in the level of service across the courts still exist. Anecdotal evidence was provided that some court staff will not speak with police staff and that faxes or e-mail should only be used. In these instances, the staff reported that it is quite common for the query to remain unresolved for some time.

2.4.1.3 HMIC Auditors are of the opinion that through the LCJB, the Force should continue to work with the courts to remove the inconsistencies that are being experienced. This could provide a further opportunity to discuss any deficiencies in processes that may exist between the courts and the police when queries arise, in order to improve the exchange of information between both agencies.

2.4.2 Relationship with non police prosecuting agencies (NPPAs)

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

therefore encourage the Force to introduce Service Level Agreements with its NPPAs to achieve this.

- 2.4.2.2 The force currently reacts to the lack of information from NPPAs by updating the PNC when the case appears on a court register. Alternatively, when the force is asked to provide previous convictions for an offender to an NPPA, the printed record is only provided once the NPPA has submitted the appropriate source document (NPA1). Whilst this contributes to improved performance, lengthy delays could still occur between the original date when an offender was reported or summonsed, and when PNC is updated. Each NPPA should be encouraged to provide the information in a timely manner, however, without an SLA to supplement the process, there is no requirement for the NPPA to respond in terms of improving timeliness.

Recommendation 10

Her Majesty's Inspector of Constabulary recommends that the force consider the introduction of Service Level Agreements with Non-Police Prosecuting Agencies for the timely submission of data.

2.5 Processes

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

- 2.5.1.1 On 1st January 2005, the performance indicators of the ACPO Compliance Strategy were replaced by the timeliness standards contained within the newly published Code of Practice for the PNC. The PNC Code of Practice, developed by the National Centre for Policing Excellence (NCPE) and endorsed by ACPO, is a statutory code made under s.39a of the Police Act 1996 (inserted by section 2 of the Police Reform Act 2002). The Code stipulates that 90% of recordable offences be entered onto PNC within 24 hours of the commencement of proceedings. The commencement of proceedings is defined as when a person is arrested, reported or summonsed.

- 2.5.1.2 The creation of arrest/summons (A/S) reports in Devon and Cornwall is a semi-automated process using an interface between the Force's Criminal Intelligence System (CIS) and the PNC. When an offender is taken into custody, a record, equivalent to a full record on the PNC, is created on CIS. A hard copy of the record is faxed to the Force National Computer Bureau (FNCB) at Force headquarters where staff quality assure the faxed record against the record on CIS. Once the quality assurance is complete, staff in FNCB create what is known as a 'process record' for each A/S report, which then enables the subsequent transmission of the record to the PNC via the Force interface.

- 2.5.1.3 In addition to the faxed form, the FNCB also require a hard copy of the original form to be sent through the internal mail system. This is used as

a fail safe to ensure that all arrestees that require an update to PNC are notified to FNCB within the required 24 hour time period. However, HMIC Auditors are of the opinion that the current process is paper intensive and due to the natural delay in receiving the original form via the internal mail system, which can take up to two days to arrive, any records that are identified as falling outside the required timeliness standard would not be captured quick enough. Furthermore, using statistics that are generated by the Force, during May 2006 only 2% of source documents fell outside of the timeliness standard (67 forms out 3,335), therefore, HMIC Auditors consider that there scope for an improvement to the process to remove some of the current bureaucracy, without affecting overall performance.

2.5.1.4 However, whilst there is scope to remove the volume of paper flow between the custody suites and the FNCB, the Force should not remove any function that provides a facility to ensure that all forms have been submitted. If the hard copy of the source documents can be removed from the process, the Force should consider placing responsibility for ensuring that all source documents are submitted with either the staff in the custody suite or with staff in FNCB. The custody system enables interrogation of records and can be used to determine whether all records that require a PNC update have had a fax sent to FNCB. If custody suites are given this responsibility, the staff already have the skills on the system to complete interrogation quickly and any failures that have occurred in relation to the faxing of documents can be identified quickly and resolved quicker in order to achieve the timeliness standard.

2.5.1.5 Another aspect of the process surrounding the creation of A/S reports that is worthy of note within this report is that of Penalty Notices for Disorder (PNDs) that are issued on the streets by operational officers. In contrast to PNDs that are issued within the custody suites, when the normal process is used, street issued PNDs result in a fixed penalty notice being produced and the offender does not have to attend the police station. During interviews and focus groups, HMIC auditors discovered that whilst officers were aware of the correct process for having records updated on the PNC, they were not aware that PNDs are subject to the same timeliness standards as all other PNC updates. As a result, the same urgency is not applied to the PNDs when faxing records to the FNCB. Unlike other arrests where a record is created on CIS and the source document is faxed to FNCB to facilitate the electronic transmission of a record, PNDs are manually updated on the PNC by FNCB staff upon receipt of a faxed copy of the fixed penalty notice (FPN). Furthermore, HMIC auditors discovered that in addition to faxing FNCB, officers are also required to send a copy of the FPN to the Central Ticket office and the Crime Input Bureau to record the details of the offence on their respective IT systems. Again, this process is paper intensive for the operational officer and the Force is encouraged to review the process in order to remove any bureaucracy for the operational officer and reduce the time spent away from operational duties.

Recommendation 11

Her Majesty's Inspector of Constabulary recommends that the Force reviews the current process of faxing and submitting hard copy source documents to the FNCB in order to reduce the volume of paper flow between operational staff and the FNCB. The Force should also consider alternative methods of ensuring that all source documents are faxed to the FNCB without the need for the hard copy of the document to supplement the fax.

2.5.2 Update of court information

2.5.2.1 The Force currently updates all relevant data from the court registers onto the PNC, including disposals, remands, adjournments and bail conditions. HMIC auditors recognise this as good practice in ensuring that records are not only accurate but complete for the benefit of the Force and all other forces who may have reason to access the records that are updated by Devon and Cornwall Constabulary.

2.5.2.2 However, HMIC Auditors are concerned that the current processes employed for updating court results are inefficient and placing a drain on the resources. The Force is currently triple keying all data from the court registers onto IT systems, with the same updates being made to PNC, NSPIS Case Preparation and CIS. HMIC auditors acknowledge that the NSPIS Case Preparation has recently been implemented and that a transition needs to be made, however, the force should consider what benefits are being achieved through this 'triple keying' process. Any opportunities to remove inefficiencies and duplication of effort must be prioritised in order to gain maximum use of resources.

2.5.3 Originator Line

2.5.3.1 The originator line on the PNC is a free text field of 72 characters that is used to provide an explanation and reference for all PNC transactions. The originator line can be used to assist the investigative capabilities when enquiries are made on the system using the #TE transaction. The #TE provides details of historic transactions against PNC records and can help investigators identify movements of subjects or vehicles if they have been checked in other force areas.

2.5.3.2 Within Devon and Cornwall Constabulary, the correct updating of the originator line is embedded within Force policy which states *"Accurate records of transactions must be made which identify the persons responsible for handling and making the request for information. In addition, the location of the check must be recorded as well as the reason for the check being carried out. The facility to record this is presented to the operator each time a check is carried out."*

2.5.3.3 However, during reality checks, HMIC Auditors selected a random sample of 98 transactions that had had been carried out on two

separate days at the beginning of July 2006. Of the sample taken, 22 records (23%) did not conform to the force policy. Examples of mistakes included lack of a reason for the check, incomplete location and no reference. Therefore, it is the opinion of HMIC auditors that in order to improve the investigative capabilities of the system, the Force should reinforce the current policy for accurate completion of the originator line.

2.5.4 Ad hoc intelligence updates⁹

2.5.4.1 In Devon and Cornwall if CIS is updated with ad hoc intelligence updates the PNC record will only be updated if the CIS record has an outstanding impending prosecution. Consequently, the risk is that the CIS record could have the most recent information on the offender rather than the PNC record. A recent internal data protection audit also identified this as a risk.

Recommendation 12

Her Majesty's Inspector of Constabulary recommends that the Force introduce a procedure to update the PNC with ad hoc intelligence recorded on the CIS application to improve the quality of the information on the system.

2.5.5 Data Quality

2.5.5.1 HMIC Auditors conducted reality checks of records that have been updated by Devon and Cornwall Constabulary to determine the quality of data being supplied by officers and subsequently input to PNC. This was achieved by obtaining a sample of source input documents as well as a sample of court registers and reviewing them against the corresponding record on the PNC. HMIC Auditors also carried out a Vehicle On-Line Descriptive Search to find all Information and Lost/Stolen Reports that had been updated on vehicles by the constabulary on a particular date.

2.5.5.2 HMIC Auditors were pleased to note that the quality of information held on the PNC was an area of strength for the Force. During the reality checks, no significant errors were found and only a small number of minor typographical errors were discovered. The results are based upon a stringent quality assurance regime within the Force where in some cases, 100% of updates are checked. In addition, the force records all details of the quality assurance in order that records of staff performance can be kept. These are then used within the appraisal system that the Force uses for the development of the staff. HMIC auditors consider the recording of such checks to be good practice.

2.5.5.3 However, HMIC Auditors are also of the opinion that whilst the quality assurance regime is robust, the system of checking 100% of updates can be excessive and contain inherent risks. The force should consider carrying out the quality assurance using a risk based approach in order to gain maximum use of resources. In the case of updates made within

⁹ Information applicable for update to PNC that originates from a source other than the creation of an Arrest/ Summons report.

FNCB where the error rate is very low, 100% checks are not required and the Force may benefit by changing to a dip sample approach. One of the risks associated with 100% checks is that staff making the updates know that all work is being checked, therefore, there is a risk that complacency will develop. If a dip sample approach was to be considered, staff would not know whether records are going to be quality controlled and are therefore more likely to ensure care is taken to maintain accuracy, particularly if the results of the quality assurance are to be used within the appraisal system.

Recommendation 13

Her Majesty's Inspector of Constabulary recommends that the Force considers the current volume of quality assurance in order to develop a risk based approach to maximise the current resources.

2.5.6 Impending Prosecutions

2.5.6.1 During the inspection, HMIC Auditors examined the process for ensuring that all outstanding prosecutions that are twelve months old are legitimately outstanding.

2.5.6.2 The PNC Liaison Officer in FNCB receives a printed list of impending prosecutions on a monthly basis from Hendon Data Centre. The list is broken down by BCU and sent out to the relevant Results and Convictions Unit (R&C). Staff in the R&C units research the cases and update the results on PNC as necessary. Where a case is legitimately outstanding, the CIS record is appended with the most up to date information in order to reduce the risk of any duplication of effort when future lists arrive from the PNC Liaison Officer. The results of this process are provided in more detail in paragraph 2.6.3.

2.6 Results

2.6.1 In June 2006, Devon and Cornwall Constabulary input 85% of Arrest/Summons (A/S) updates on PNC within 24 hours. This shows a slight increase in performance in the 12 months from June 2005 when 81.9% of cases were input within 24 hours. Despite a large drop in November 2005 when only 66% of cases were input within 24 hours, performance has remained relatively static with the Force achieving between 80% and 85% in most months. Current performance is just below the national average for England and Wales of 86.1%. In terms of the number of days to enter the quickest 90% of cases, the Force was taking 4 days in June 2006, just outside of the target. This performance is also a slight improvement over the twelve month period, with 90% being achieved in 6 days in June 2005. The current performance in the terms of the number of days to achieve the target is slightly better than the national average of 5 days for England and Wales. However, HMIC Auditors are of the opinion that performance can be improved when the Force implements a change to the CIS system which will allow the Force to differentiate between its own records and those of Non-Police

Prosecuting Agencies, a facility that all other forces have enjoyed for over twelve months already.

- 2.6.2 In terms of disposals, statistics show that the Force is currently performing in the top 5 of the 43 forces in England and Wales. In June 2006, 88.4% of cases were updated within 10 days, against a target of 75%. This rate of performance has been consistent for the last six months and is a slight improvement on the June 2005 when 85.7% of cases were entered within the target time. With regards to the number of days to enter 75% of cases, the force currently achieves this in 6 days against a target of 10 days. In relation to both measurements, the Force is achieving performance levels in excess of the national average for England and Wales of 66.9% and 37 days respectively.
- 2.6.3 Finally, with regard to outstanding prosecutions on the PNC in the 12 months to June 2006 the Force has shown an overall increase in the number of outstanding cases of 23%, rising from 3,874 in June 2005 to 4,780 in June 2006. However, this increase coincides with the commencement of the powers under the Criminal Justice Act 2002 whereby all arrestees are updated on the PNC. In April 2001, HMIC supported by the Home Secretary stated that all forces should be in a position to confirm that any outstanding case that is over twelve months old, is legitimately outstanding and that no more than 75.4% of cases should be older than twelve months old. In Devon and Cornwall, despite the increase in the overall number of cases, 92.8% of cases remain within the twelve month age bracket, maintaining their position within the profile. HMIC Auditors are therefore assured that the Force is able to provide such confirmation.

APPENDIX A**SUMMARY OF RECOMMENDATIONS FOR DEVON and CORNWALL****Recommendation 1**

Her Majesty's Inspector of Constabulary recommends that the terms of references for the group be updated to include the statutory code of practice for PNC. The group should also consider timings the meetings to align with regional/national groups.

Paragraph 2.1.1.3

Recommendation 2

Her Majesty's Inspector of Constabulary recommends that the Force ensures that PNC Performance is considered as a standing item in the self-assessment process of the Criminal Justice Department.

Paragraph 2.1.2.4

Recommendation 3

Her Majesty's Inspector of Constabulary recommends that the Force develop a strategic action plan to support the delivery of the aims and objectives contained within the PNC Strategy. The action should be dynamic to reflect the changing face of the PNC and be owned and managed by the PNC Steering Group.

Paragraph 2.2.1.3

Recommendation 4

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

- Introduces a policy and process to ensure that only staff who require PNC access as part of their role are provided with access to the system;
- Introduces an independent audit, at least annually, of all user access administration

Paragraph 2.2.2.8

Recommendation 5

Her Majesty's Inspector of Constabulary recommends that the Data Protection Unit commence a process of dip sampling returns from line managers in respect of transaction monitoring.

Paragraph 2.2.2.11

Recommendation 6

Her Majesty's Inspector of Constabulary recommends that the Force consider options for the proactive monitoring of PNC activity.

Paragraph 2.2.2.15

Recommendation 7

Her Majesty's Inspector of Constabulary recommends that the Force should examine ways of improving the levels of awareness of each aspect of Information Management amongst all staff. Consideration should be given to ensuring that the current mandate is adhered to in order that the current response rate of 15% is improved.

Paragraph 2.2.2.18

Recommendation 8

Her Majesty's Inspector of Constabulary recommends that the Force develop a programme of awareness presentations targeted at uniformed staff and supervision. The force should also consider the use of internal marketing experts to exploit further opportunities to raise the levels of awareness amongst staff of both PNC and ViSOR.

Paragraph 2.3.1.6

Recommendation 9

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

- Immediately cease the training of PNCB and Records and Convictions staff by non-accredited trainers;
- Introduce formal assessment processes on all PNC courses, ensuring that they are evidence based and comply with PICTTS Occupational Training Standards;
- Consider the benefits of enhancing the training evaluation for PNC courses by introducing post-training evaluation.

Paragraph 2.3.2.8

Recommendation 10

Her Majesty's Inspector of Constabulary recommends that the force consider the introduction of Service Level Agreements with Non-Police Prosecuting Agencies for the timely submission of data.

Paragraph 2.4.2.2

Recommendation 11

Her Majesty's Inspector of Constabulary recommends that the Force reviews the current process of faxing and submitting hard copy source documents to the FNCB in order to reduce the volume of paper flow between operational staff and the FNCB. The Force should also consider alternative methods of ensuring that all source documents are faxed to the FNCB without the need for the hard copy of the document to supplement the fax.

Paragraph 2.5.1.5

Recommendation 12

Her Majesty's Inspector of Constabulary recommends that the Force introduce a procedure to update the PNC with ad hoc intelligence recorded on the CIS application to improve the quality of the information on the system.

Paragraph 2.5.4.1

Recommendation 13

Her Majesty's Inspector of Constabulary recommends that the Force considers the current volume of quality assurance in order to develop a risk based approach to maximise the current resources.

Paragraph 2.5.5.3

APPENDIX B**SUMMARY OF GOOD PRACTICES AT DEVON and CORNWALL**

- Statistics in relation to submission of Source Documents for the creation of arrest/summons reports are produced on a monthly basis and broken down by BCU. When errors on the forms occur, the types of error are also recorded.
- Policies are stored electronically on a database which includes a prompt to ensure that all policies are reviewed on a regular basis.
- The internal messaging system on the command and control system is used for issuing transaction monitoring checks, ensuring that validation of the checks occurs as soon as practicable after the transaction has been made.
- Professional Standards have their own PNC research capability and when other staff within the force are required, a confidentiality contract is used to protect the nature of the investigation.
- Student Constables on the Initial Police Learning & Development Programme (IPLDP) receive a comprehensive input relating to the PNC.
- The force updates a full record at source and also updates the PNC with all relevant information from court registers, including adjournments and bail conditions.
- Statistical Information is recorded pertaining to the quality control of data that has been input to PNC by within the force. The statistics are then used as part of the staff appraisal system.

APPENDIX C – ‘ON THE RECORD’**THEMATIC INSPECTION REPORT ON POLICE CRIME RECORDING, THE POLICE NATIONAL COMPUTER AND PHOENIX INTELLIGENCE SYSTEM DATA QUALITY - RECOMMENDATIONS****Recommendation 9** (Chapter 5 page 86)

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

Recommendation 10 (Chapter 6 page 104)

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

Recommendation 11 (Chapter 7 page 111)

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

Recommendation 12 (Chapter 7 page 112)

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

Recommendation 13 (Chapter 7 page 118)

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

Recommendation 14 (Chapter 8 page 145)

Her Majesty's Inspector recommends that Forces ensure that each Phoenix inputting department develops an audit trail to register the return of substandard PSDs, via line supervisors, to originating officers. The system developed should include a mechanism to ensure the prompt return of PSDs. Forces should also incorporate locally based audit trails, monitoring the passage of returned PSDs between line supervisors and originating officers.

Recommendation 15 (Chapter 8 page 146)

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

Recommendation 16 (Chapter 8 page 148)

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

Recommendation 17 (Chapter 8 page 150)

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

Recommendation 18 (Chapter 9 page 164)

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

Recommendation 19 (Chapter 9 page 164)

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

Recommendation 20 (Chapter 9 page 165)

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

APPENDIX D – PRG REPORT**“PHOENIX DATA QUALITY” RECOMMENDATIONS**

- National performance indicators and standards for timeliness of input, data fields to be completed, quality assurance requirements and the provision of training should be agreed by ACPO and promulgated to all Forces.
- Achievement against and compliance with these indicators should be audited after a period of 12 months, perhaps through the inclusion in the scope of HMIC audits.
- Senior officers take an active and visible role in policing compliance with agreed standards within their own Force.
 - ACPO performance indicators should be reflected in Force policy or standing orders (or the Force equivalent). Guidance should include the responsibilities of officers at each stage of the process e.g. for the provision of source documentation, for approval, time taken to pass to input bureaux, and the bureaux' responsibilities for data entry and quality control.
 - Line and divisional managers, as well as chief officers, should be held accountable for compliance with these standards. This could be achieved through inclusion in divisional efficiency assessments, and through the publication and dissemination of performance statistics throughout individual Forces and nationally.
- Source documentation should be common across all Forces, if not in design, in the information requested. A national format, stipulating a hierarchy of fields to be populated, should be developed.
- Programme(s) geared to raising awareness amongst operational officers and line managers of the potential benefits of Phoenix in a practical sense and their responsibilities of the provision of data should be developed. To ensure all officers have an opportunity to benefit from these programmes, consideration should be given to inclusion of a 'Phoenix awareness' module in probationer training, promotion courses and divisional training days.
- Best practice in administrative arrangements and organisational structures should be widely distributed. Internal working practices and organisational structures should be streamlined to remove any redundancies.

- Greater computerisation of the transfer of results from courts direct to Phoenix should continue to be developed. In the shorter term, the Police Service is likely to retain responsibility of the input of court information. To minimise the resource burden on the Police Service in this interim period, the police and courts should work to ensure recognition of each other's requirements and to minimise any inconsistencies in their respective working practices.
 - In the first instance, this might be achieved by ACPO highlighting to Magistrates' Courts and to the Crown Court, perhaps through the Trials Issue Group, the importance of Phoenix records to the integrity of the criminal justice system as a whole. Liaison meetings could usefully be established to introduce greater consistency in working and recording practices between the courts and police Forces e.g. for recording data. In the first instance, this could be pursued locally, perhaps through the court user group. Issues considered by such meetings might include supplying additional information (such as Arrest / Summons numbers) to the Magistrates' Court system and to automated transfer of court registers.
 - Consistent practice and performance is also required from the courts. Recommendations referring to performance indicators and standards, audits and monitoring, senior level commitment, common recording practices, awareness of system customers and administrative 'best practice' could equally apply to the courts. Mirroring the responsibilities of Chief Constables for their Force, the Court Service and the Magistrates' Court Committee should be accountable for the performance of courts.
 - Consistent practice in advising custody details, including transfers and releases, is required. This includes consistency in advising CRO numbers to maximise the number of complete records. The police and prison services should liaise to encourage greater understanding and acknowledgement of each other's requirements.

APPENDIX E – 1ST PNC REPORT**POLICE NATIONAL COMPUTER DATA QUALITY AND TIMELINESS –
RECOMMENDATIONS****Recommendation One (Paragraph 5.2)**

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

Recommendation Two (Paragraph 5.11)

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

Recommendation Three (Paragraph 5.19)

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

Recommendation Four (Paragraph 5.29)

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

Recommendation Five (Paragraph 5.31)

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

Recommendation Six (Paragraph 5.34)

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

Recommendation Seven (Paragraph 6.10)

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

Recommendation Eight (Paragraph 6.12)

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

Recommendation Nine (Paragraph 6.14)

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

Recommendation Ten (Paragraph 6.16)

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

APPENDIX F – 2ND PNC REPORT**POLICE NATIONAL COMPUTER DATA QUALITY AND TIMELINESS –
RECOMMENDATIONS****Recommendation 1**

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

Recommendation 2

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

Recommendation 3

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

Recommendation 4

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

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

Recommendation 5

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