APPENDIX 1

MPS PNC STEERING GROUP RESPONSE

to the

Report by Her Majesty's Inspectorate of Constabulary

'ON THE RECORD'

1. Recommendation 9

HMI 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. It 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.

The Police Research Group (PRG) Report

1.1 The MPS Police National Computer Bureau considered the recommendations of the 1998 PRG report relating to Phoenix Data Quality, and working practices were changed to comply. The MPS is addressing the key actions as per the ACPO Compliance Strategy, and is integrated in the action plans detailed later in this response for the recommendations made by HMI.

ACPO Compliance Strategy 'Key Actions'

1.2 Comply with the National Police Information Management Strategy (IMS) and PNC Compliance Strategy action plans.

1.3 The MPS Strategy and Operational Support Group [DCC10(2)] delivered the new MPS Information Strategy (IS2K) on 22 December 2000 according to plan. This strategy directly supports the ACPO National Police Information Management Strategy. Planning is already underway within the Directorate of Information to plot the necessary work packages that will enable the MPS to migrate from existing information systems to the new information architecture described within the ACPO and IS2K Strategies.

1.4 Be aware of and comply with the ACPO Data Protection Audit Manual and other system manuals. When new systems are developed, they should be used according to the operating rules provided.

1.5 The MPS Service Security Branch [PRS2(2)] is fully aware of the ACPO Data Protection Audit Manual. All inspections are conducted to comply with the manual and, where appropriate, are extended to identify additional areas of quality.

See also HMIC 'On the Record' Recommendation 18.

1.6 Ensure that appropriate staff is selected for PNC training and, where suitable, apply the national competency profile (generated by the National Police Training) and train to the national standards where these have been set.

1.7 *See HMIC 'On the Record' Recommendation 13*.

1.8 Establish the present level of resources committed to gathering, collating, inputting and using data and determine the level required to achieve the principles in the IMS. The performance indicators (P.I.s) proposed may assist in defining the levels of resources required and the appropriate competencies those staff will need.

1.9 The level of resources required to fulfil the obligations of the IMS and P.I.s are currently being reviewed taking into account future I.T. projects (NSPIS Custody and Case Preparation). The MPS is in the process of rolling out a new IT system for updating court results. This should be completed by September 2001. The work being conducted on recommendations 14 and 15 will be used to assist in determining the resources required. This will need to incorporate best value and good practice.

1.10 Establish levels of awareness amongst senior staff in the capabilities of PNC/QUEST/CCA/VODS and ensure that the full potential of these national systems is appreciated.

1.11 The MPS PNC Steering Group is defining a new PNC marketing strategy, which will be fully implemented once all the features affected by the recommendations have been defined.

See also HMIC 'On the Record' Recommendation 11.

1.12 Establish robust quality assurance processes in line with the IMS action plans.

1.13 Planning is under way within the Directorate of Information to plot the necessary work packages (including QA processes) that will enable the MPS to migrate from existing information systems to the new information architecture described within the ACPO and IS2K Strategies.

1.14 Ensure reporting lines exist to allow Data Protection Officers to raise matters at a senior level.

1.15. The MPS Data Protection Officers are established members of the MPS Security (METSEC) Program Board, Performance Review Group (PRG) and MPS PNC Steering Group, which enables them to raise issues at the highest level.

1.16 Ensure that internal Best Value and performance reviews focus on optimum use of data and compliance to standards and make clear links between effective data management and operational performance.

1.17 The MPS PNC Steering Group is determining the most appropriate mechanism for achieving this action. However, it cannot be tackled until the question of the MPS IT Training Schools accreditation by National Police Training is resolved. (See supporting discussion in para 4 Recommendation 13).

1.18 Establish the reason for their performance against national P.I.s and take action where appropriate.

1.19 The MPS's statistics for the National Performance Indicators have been studied and areas of potential improvement are being identified along with additional in depth statistics to increase the ability to identify weak key processes. Any proposed changes will be considered against known future I.T. developments before implementation.

1.20 Recognise the importance of the Phoenix Source Document. Periodic reviews of the submission process should be carried out to ensure efficiency.

1.21 *See HMIC 'On the Record' Recommendations 14 and 15.*

2. Recommendation 11

HMI recommends that the marketing, use and development of national police information systems are integrated into appropriate Force, local and departmental, strategic planning documents.

2.1 The MPS PNC Steering Group has identified appropriate strategy and co-ordination groups within the existing MPS structure to promulgate the benefits available from extensive use of the PNC as an investigative and record keeping tool. The MPS IT Training School already have a direct input to CID training courses to promote awareness of the facilities offered by PNC and its use as an investigative tool. Additionally, staff from the MPS PNC Bureau, supported by PITO, gives presentations throughout the organisation, including the SIO courses.

2.2 Direct lines of communication will be developed between these groups and the MPS PNC Steering Group to facilitate awareness of National Police Information Systems (PNC) and their integration into force, local, and departmental strategy and planning procedures. The PNC Marketing Strategy will directly support this approach. The target date for publication is the end of 2001.

3. Recommendation 12

HMI 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.

3.1 The MPS has established a PNC Steering Group under the chairmanship of a Deputy Assistant Commissioner to co-ordinate actions, including issues arising from the HMIC 'On the Record' report. The group is responsible for the MPS PNC Strategy and other related information management issues.

(See annex A for the Terms of Reference).

3.2 The membership of the group will be extended to assist, where appropriate, the recommendations of the HMIC 'On the Record' report.

4. Recommendation 13

HMI recommends that all Forces conduct an audit of their present in-force PNC trainers to ensure that 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.

4.1 The Information Technology Training School at Hendon (P9(5)) is an authorised training establishment that has been training MPS personnel in PNC for over twelve years. During this time, there have been no issues of concern surrounding the MPS's use of PNC that are directly related to the quality and standard of training provided.

4.2 The MPS IT instructors within P9(5) are experienced and skilled in the use and instruction of PNC, having come from an operational background where using the system was part of their daily duties. Instructors undertake a four- week foundation course, followed by a monitored development plan with two formal classroom-based assessments on their return to the workplace. Within six months, they are required to attend a two-week Trainers Development Course. From their first training day, instructors are required to maintain a skills and competency portfolio under the Training Design Lead Body standard format, which is regularly checked by the P9(5) Staff Development Officer and Head of IT Training. As part of this process, they must undergo at least four assessments in their first year and two annually after that to NVQ standards. In addition, all instructors either have or are working towards the Certificate in Education and may have extended their course to earn MAs. ***This programme has previously been acceptable as the national standard for all IT training***.

4.3 The IT Training School currently has twenty PNC instructors, training all Command and Control personnel in PNC usage. Last year, 600 MPS personnel were trained in the use of PNC. Additionally, P9(5), on behalf of SO3 PNC Bureau, also trains to deliver 'PNC on OTIS' trainers who are delivering training within the workplace. None of these instructors has attended the NPT PNC trainers' course and, therefore, under HMIC's definition, are no longer authorised to conduct in-force PNC training.

4.4 The impact of introducing the requirement in this recommendation would be significant and have major implications for the MPS. Whilst there are a large number of trained personnel within the organisation, many are not available for deployment within control rooms. The MPS has recently embarked upon a major civilian recruitment programme for Communication Officers. Were they not to be trained in PNC by the current instructors, they would be unable to fill their role within the control room environment. Additionally, the inability of local trainers to train 'PNC via OTIS' would impact on the control rooms by driving back into those rooms the 'non-operational' PNC checks that PNC via OTIS was designed to remove from that environment. Equally, the use of Mobile Data Terminals allows officers to interrogate PNC remotely. Narrowing the ambit of training to specialist control room operators would deny the MPS a huge business benefit.

4.5 The MPS view is that to adhere to this recommendation by sending in excess of 200 existing trainers to attend the 3-week NPT trainers' course at Leicester is

logistically impossible. Additionally, it does not make business sense when the MPS have an efficient training facility in-force. ***The MPS believe there is a need for mediation and would suggest that the Information Technology Training School at Hendon be accredited by National Police Training to deliver PNC Instructors courses.***

5. Recommendation 14

HMI 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 audits trails, monitoring the passage of returned PSDs between line supervisors and originating officers.

Recommendation 15

HMI 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.

5.1 These recommendations will be dealt with together, as they are directly related under one action plan.

5.2 The current PNC Source Input Document (PSID) rejection procedure has been extended to record the completing and supervising officers' details. The rejections will be channelled back to the officers concerned through the OCU Criminal Justice Unit Managers. This system is being designed for implementation by September 2001.

5.3 A full review will be conducted of the PSID submission procedure in conjunction with the Criminal Justice Office. Once completed, policy documentation will be updated and disseminated through the Marketing Strategy. (Timescale end 2001)

5.4 A general data and PSID docket quality check procedure will then be developed to highlight areas of concern raised in the HMIC 'On the Record' report. This will include the reason for procedure and the actions to be taken by the offending officer.

5.5 The development of this new procedure will be linked to a business case for additional resources for SO3(3) prior to any implementation.

5.6 A review of the policy and procedure will be conducted.

6. Recommendation 16

HMI 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 regular checks are conducted to ensure compliance.

6.1 It is proposed to utilise the OCU's Intelligence Units as one of the focal points of the PNC Marketing Strategy. This theme will continue to promote best use of PNC as an information, intelligence and record keeping system. The MPS currently has an ad-hoc update procedure for information, which becomes available outside an arrest scenario.

6.2 This system will be reviewed in conjunction with the lead branch for Intelligence (SO11) to determine a best value approach to the maintenance of PNC data from intelligence sources.

This will also feature within the review of the PSID.

7. Recommendation 17

HMI 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.

7.1 The PNC Bureau already has a number of quality assurance processes in place to validate work completed by their staff. This currently takes the form of checks performed by the operator's supervisor during the tour of duty, especially for new members of staff or after any procedural change. This is supported by a 10 % validation of all daily work. These are supplemented by unit or operator specific audits, if highlighted from other sources. Any issues highlighted by PNC Compliance audits section are also considered for specific validation.

7.2 All sections of the PNC Bureau have a Statistical Input Sheet for each operator; this is divided into different core functions and is used by line managers to monitor the performance of their staff. These and other factors are used as evidence for career development and annual appraisals.

8. Recommendation 18

HMI recommends, where not already present, that Forces develop risk assessed Force Data Protection Officer audit programmes.

8.1 A risk assessment has been conducted in accordance with the methodology recommended by the HMIC. A programme of audits has been drawn up to address those functions that appear to present the greatest risks. Resources have been allocated under the management of the Data Protection Officer.

8.2 This process will be reviewed in the light of any significant changes to the PNC system or working practices.

9. Recommendation 19

HMI recommends that Forces integrate PNC and Phoenix data quality compliance into their performance review and inspectorate programmes for BCUs and specialist departments.

9.1 In conjunction with the work carried out under recommendation 14 and the MPS PNC Marketing Strategy, the MPS PNC Steering Group will liaise with the Performance Review Unit to incorporate data quality and compliance within the review and inspection processes.

10. Recommendation 20

HMI 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.

10.1 The actions under recommendations 14 and 15 will be utilised to produce statistical information in support of this recommendation and will be introduced in consultation with the Performance Review Unit. The level of information required might have resource implications for SO3(3), which will need to be addressed prior to any implementation.

MPS PNC STEERING GROUP

TERMS OF REFERENCE

- To co-ordinate all PNC activities in the MPS

- To promote investigative capabilities of PNC

- To promote and maintain the submission and input of high quality data on PNC

- To act as a channel for consideration of PNC policy

- To encourage and promote the spread of formal training of PNC applications

- To promote the development of PNC to support the delivery of MPS operational priorities

- To consider security, data protection and quality control issues in relation to PNC and oversee audit and monitoring processes to satisfy relevant codes of practice, connection, etc.

- To oversee the roll out of PNC systems, access and security within the MPS

- To conduct an impact analysis on national policy and promulgate best practice

MPS PNC Steering Group Secretariat
SO3(3) Policy & Planning Unit
Room 130, New Scotland Yard
Metphone 60645 or 62792