1 Who you are and a brief summary of your career history?

I am employed by the National Policing Improvement Agency (NPIA), a Non Departmental Public Body of the Home Office. The NPIA, by way of background and purpose, is a national organisation created to support effective policing and improve public safety. The agency provides critical national services that directly support frontline policing such as the Police National Computer (PNC), Automatic Number Plate Recognition (ANPR), the National DNA Database and Proceeds of Crime. The agency also delivers training and leadership development to improve the expertise in police forces and police authorities, shares evidence-based research and good practice to promote and improve policing and provides support to the police service in the use of technology and procurement.

I have over 35 years public sector experience, and my career in Information Technology began in 1980 with the Department for Employment. In 1995/7 I worked on the Job Seekers Allowance Project before moving to Home Office as Head of Software Development for PNC (1997 – 2000) at the Hendon Data Centre. In 2000 I took on the role of National Service Manager for National Strategy for Police Information Systems (NSPIS) based in central London, returning to Hendon to run the PNC Services Software Development Team in mid 2005.

In September 2007 I took on the role of Head of PNC Services which includes responsibility for the PNC and a number of other national information systems that are provided to UK Police Forces and other Criminal Justice Organisations.

In 2011 I assumed additional responsibility for the NPIA Information Services portfolio with over 100 staff bringing the total number of staff under my control to just fewer than 300, which includes teams of multi-disciplinary technicians, IT service management, customer service and administrative staff. I am based at the NPIA Hendon Data Centre in North London.

2 What is the police national computer?

The PNC, is a major operational tool and is used to record convictions, cautions, reprimands and warnings for any offence punishable by imprisonment and any other offence that is specified within regulations. The PNC is maintained by the NPIA and is used by all police forces in England and Wales to carry out their policing duties.

A Home Office document, circa 1980, that I have access to states "*The aim of the Police National Computer (PNC) is to provide a central store of*

information which can be rapidly interrogated and updated by terminals situated in every police force. This information will comprise a number of national indexes relating to crime and criminals together with other information of interest to the police such as details of vehicle ownership. The information will be available to all police forces twenty four hours a day and is designed to be the minimum required for immediate operational action by the police." This, to me, provides the business perspective of what PNC is.

The PNC was established in 1974 and has evolved over time to link a number of separate databases. It holds a range of records, including details of:

- people who are convicted, cautioned, arrested, wanted or missing;
- the registered keeper of vehicles;
- people with a driving licence entitlement or who are disqualified;
- certain types of stolen and recovered property including animals, firearms, trailers, plant machinery and engines and also supports enquiries against the National Phone Register;
- people on the National Firearms Certificate Holders register.

The PNC links with a number of other systems: ViSOR (Potentially Dangerous Persons database); Motor Insurance; Support for ANPR and Support for Airwave Radios. The National DNA Database (NDNAD) and Ident1 (National Fingerprint Database) are also linked to the PNC. Work is underway to link it to the Schengen II system (Schengen will provide details of people and property being sought by any state that is a signatory of the EU treaty who can access the system).

The PNC is an information system used by all police forces in the UK and other authorised agencies. It is currently hosted on a mainframe computer, a Fujitsu S200 Business System to be precise, which was commissioned in March 2010. It uses a programming language known as Natural and database management system known as ADABAS.

The PNC is available 24x7 and is part of the UK's Critical National Infrastructure. It is a very resilient system with demonstrably high levels of availability, for example 99.96% 2011/12 to date against a target of 99.5% and has consistently provided similar levels of service over the last five years and beyond.

It has in excess of 250,000 users and in recent years has handled in excess of 169 million transactions (a check or update of a record) per annum, giving a daily average of just under 463,000 transactions. It makes extensive use of logging all enquiries and updates - this functionality facilitates the auditing and police investigations.

It is hosted at NPIA Hendon Data Centre (HDC) which is situated in North London. It has a second site within 20 miles, which can be used operationally and also provides business continuity in the event of a disaster. Both sites support the provision of 24/7 operations. Both sites meet or exceed current security requirements and have been subject to periodic external reviews.

3 What are the main categories of the information that it holds and for what purposes?

PNC is used by law enforcement agencies to both record and provide any information about individuals, vehicles, driving licences etc for law enforcement purposes including the apprehension and prosecution of offenders, the prevention and detection of crime and public protection e.g. wanted and missing people. It is required for many legitimate policing purposes, from anywhere in the UK and at anytime, facilitating national communication across all UK forces.

The PNC itself comprises four main databases:-

- **Names** (the person's details) - as at 1st January 2012, there are just over 10.4 million records. Of these, approx 9.5 million have a criminal conviction and, since 2006, when the Criminal Justice Act 2003 came in, also includes persons who have been arrested and released without charge. There are also just over 1.5 million Firearms Certificate Holders held on NFLMS. The PNC Names file includes wanted or missing persons, court orders, outstanding warrants and disqualified driver reports together with descriptive information including warning signals and information markers. The PNC is used to make this information available and shareable across all police forces and some authorised agencies.

- **Property -** Just over 75,000 records. Stolen or found property which has a unique serial number is held on PNC so that the information can be shared across all police forces. Categories of property information include Plant, Engines, Trailers, High Value Animals, Marine and Firearms. There is also a link to the National Mobile Phone Register.

- **Driver Licences -** Just over 55 million records. PNC holds a copy of all driver information held by Drivers Vehicle Licensing Agency (DVLA), again to make it readily accessible to all Police Forces.

- **Vehicles -** Just over 54 million records, providing registered keepers, current vehicle excise licence details and where applicable MOT status. PNC also holds a copy of all vehicle information for

police purposes which is supplemented by operational information e.g. vehicles of interest or stolen.

Access to Motor Insurance – PNC also provides access to Motor Insurance data relating to private motor vehicles. Police Officers can check on a vehicle's insurance by entering the Vehicle Registration Number (VRM) into PNC. The motor insurance details are held on a private database owned by the Motor Insurance Bureau (MIB) and currently hosted by their supplier Experian. All insurance companies provide their data to the Motor Insurance Bureau (MIB) which is held on the Motor Insurance database (MID).

ANPR – Police reports, known as "actions", are attached to some of the vehicle records held on PNC. The vehicle registration number of these and other details such as, priority and purpose are dynamically placed in a special area for fast access by **Automatic Number Plate Recognition** (ANPR) systems in police forces. The ANPR system checks each car's VRM, captured by its camera(s), against those held on PNC. If they match, this is known as a "hit" and the ANPR system is notified, which in turn alerts police officers to the need to take the required or specified action.

PNC can either be linked directly to other national systems, or other systems can make a call on PNC or both situations can occur. A description of these systems follows:

National DNA Database (NDNAD)

NPIA's PNC Services is also the service provider of the National DNA Database (NDNAD). PNC and NDNAD are linked together via an interface, which is used to transmit status and reference information, so the systems are kept in step. The DNA status flag (not the profile) can then be checked on PNC by the police to determine if DNA from this person has already been taken. All information relating to a profile are kept on the NDNAD together with details of any profile matches from scenes of crime.

Ident1 (National Fingerprint Records)

Fingerprint records are retained on the Ident1 database. Ident1 is linked to PNC via an interface, which is used to transmit the fingerprint status flag and reference information so the systems are kept in step and the Fingerprint status flag on a person record is known to police officers making enquiries on PNC. [Note: England, Wales and Scotland are already on Ident1. The Police Service of Northern Ireland (PSNI) is in the process of moving their fingerprint records on to Ident1]. More recently fingerprints can also be searched using a system known as mobile-id,

which is designed for checking the identification of individuals from mobile devices, for example in a police vehicle.

ViSOR (Potentially Dangerous Persons Database)

NPIA's PNC Services is the service provider of the Potentially Dangerous Persons database (**ViSOR**). This database system came into being in 2003 and is linked directly to PNC. It holds confidential data on both potentially dangerous people and sex offenders, to aid the police and probation service in managing such individuals. It also holds details on individuals subject to Control Orders in support of counter terrorism. ViSOR is a multi-agency tool and is used by police, probation and prison staff. Users can access PNC records from it. In addition certain data relating to the status of offenders' records is maintained on PNC to alert users of PNC to an individual's ViSOR status. All UK police forces now use this system.

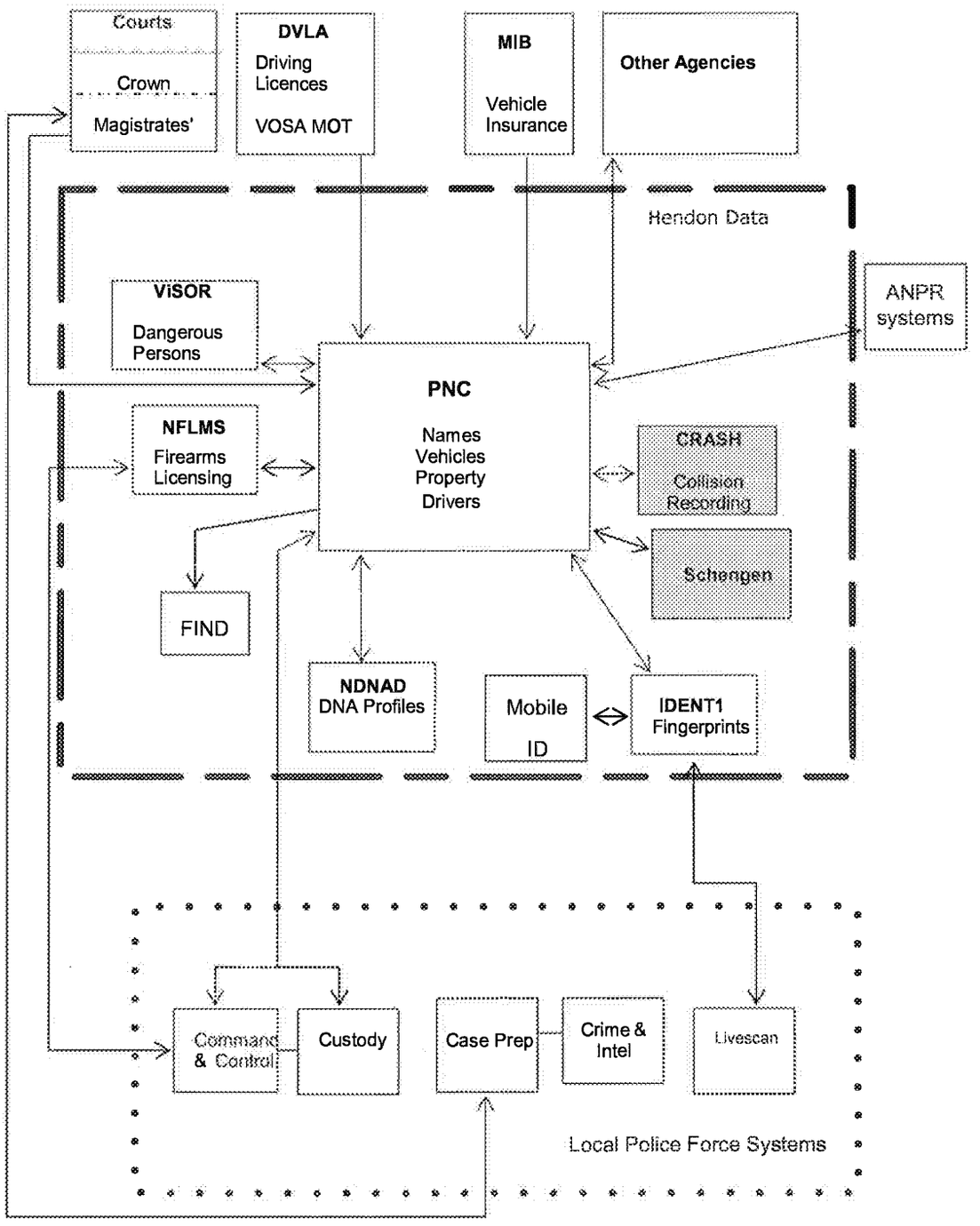
National Firearms Licensing Management System (NFLMS)

NPIA's PNC Services is also the service provider of the National Firearms Licensing System (**NFLMS**). This system came into being in 2006 following a recommendation in the Cullen Report into the tragic shooting of school children at Dunblane. It provides a national register of all registered firearms holders. The system supports the management of Firearm Certificates. NFLMS is linked to PNC to share information across all Forces on Firearm Certificate Holders for operational purposes. [Note: The system applies to forces in England and Wales. - Scotland and Northern Ireland use other systems not linked to PNC.]

Facial Images National Database (FIND)

FIND is a pilot system that holds photographs of offenders from a small number of force custody systems. It was designed to allow authorised users in the United Kingdom to access the Facial Images National Database for assistance in confirming the identification of offenders or persons of interest and aiding intelligence-led policing.

The chart shown next provides a schematic of the systems, their connections in relation to PNC and the principal information flows:



Note **CRASH**, the road collisions recording project is linked to PNC and is in the final stages of testing prior to live operation. **Schengen** will exchange data with the European law enforcement agencies from states that are signatories to the Schengen Treaty. Live operation is scheduled from 2014.

4 How does information get placed on the PNC? Who decides whether the information should be inputted?

4.1 How does information get placed on PNC

All police forces and some authorised agencies update PNC (please see PNC Service matrix documentation at Appendix 4A). Each force or authorised agency has a PNC administration section usually known as a PNC Bureau. PNC can be updated both manually i.e. through a PC (personal computer) and system to system. Force PNC Bureau usually perform manual updates for vehicles, persons and property. Many force computer systems have system-to-system interfaces to facilitate automatic checking updating e.g. custody and case preparation. Magistrate's court results are updated electronically via an interface from their Libra system directly on to the PNC. This latter development came directly from Recommendation 7 of Sir Michael Bichard's Inquiry into the Soham murders.

Information is placed on PNC and accessed in a number of different ways. Technically this is achieved by a number of different methods. The method used is primarily dependent on the specific business need. These are:-

Read and update

Directly Connected Terminals (DCT), which come direct to PNC via a connection gateway in each force.

Browser interface, which uses the same mechanism as DCT. [Not to be confused with Web Browser, this interface does not use the internet].

System to System Interfaces which enable one system to communicate directly with another. Examples include the NSPIS (National Strategy for Police Information Systems) interface between custody and PNC which is used by some forces. A derivative of the NSPIS system to system interface is also used for placing magistrate court results on to PNC.

Update only

System to System Interfaces such as Phoenix Force Interface.

And for completeness - *Read only*

Phoenix Links – This allows the Ministry of Justice (MOJ) to vet jurors, disclosure agencies such as Criminal Records Bureau (CRB) and Disclosure Scotland to read PNC records.

Airwave – PNC can also be accessed via Airwave radio systems and other mobile devices providing access to data via a gateway enabling officers to gain direct access to PNC for operational purposes. A Police Officer could use the radio to ask the control room to do a vehicle or person check or could use the radio to do so directly on PNC. Police mobile devices such as Blackberry can be similarly configured.

Additionally we have two further bespoke system to system interfaces that undertake read and update actions, as necessary, for the synchronisation of the two national databases concerned with biometrics. These are PNC to NDNAD, the DNA database and PNC to Ident1, the fingerprints database.

There are also system to system interfaces between PNC and Visor, NFLMS, and Libra.

4.2 Who decides whether the information should be input?

Data is placed on PNC in accordance with two key documents:-

- **A Home Office statutory Code Of Practice, The Police National Computer,** effective from 1 January 2005. This describes the standards that are to be complied with, for example the time periods in which data after arrests are made must be entered. This has been laid before Parliament and is in the public domain. (See Appendix 4B)
- **PNC Manual** – two significant volumes (Volumes 1 and 2) have been included here as 1 document in Appendix 4C. It describes how PNC is to be used, for example how to put records on or search records. The PNC manual is regularly updated and issued to all users electronically on a six monthly basis. More frequent instructions on use, when required, are issued through ad hoc "PNC Liaison Officer" letter.

The Code Of Practice is attached at Appendix 4B. Paragraph 23 of the code lists 12 publications relating to required actions, good practice and operating procedures in respect of the PNC.

Paragraph 24 of the code states: "In laying this code of practice before Parliament, the Home Secretary supports the continuing practice of ACPO that PNC manuals of guidance will be published, with the exception of any material in the manuals whose publication would be against the interests

of national security or could prejudice the prevention or detection of crime or the apprehension or prosecution of offenders".

To ensure that PNC is kept up to date and reflects the changing business needs of the Police Service, both legislative and business, a group structure exists to consider and prioritise the requirements. Please see Appendix 4D. This structure provides two way communications between the Association of Chief Police Officers (ACPO) and Forces. Each force reports into a *regional group*, regions being South West, South East, North West, North East, Scotland and the Midlands. Thus a change request from a force must be sponsored by the region, before it is considered nationally. *Force regional groups* feed into national user groups to cover different PNC business areas for expertise, consensus of views where possible and decisions.

PNC's governing body is the Police PNC policy and planning group (P4G). It is chaired by ACC David Pryde of Hampshire Police. P4G reports into ACPO's IMBA (Information Management Business Area) Group.

P4G uses several sub-groups to formulate proposals and recommendations for change to functionality on PNC, including the PNC Manual. The national groups are chaired by a functional expert with considerable policing knowledge. A schematic of the organisational structure can be found at Appendix 4D, and the sub-groups are shown below:-

- **The PNC Names Group** (PNG), deals with person record information.
- **Vehicles Working Party** (VWP), deals with vehicles and property.
- **Service Level Agreement Management Group** (SLAMG), deals with writing and monitoring the PNC service level agreement with police forces.
- **PNC Interface Working Group** (PIWG), deals with all issues where an interface exists into PNC such as downloading arrest information from force systems.
- **Training Working Party** (TWP), deals with PNC training standards and matters.

Ultimately, Chief Constables as data controllers are responsible for the data placed on PNC, the use to which it is put within their force and the actions of their staff.

5 Which organisations have full access to information held on the PNC? For what purposes are they permitted to access the PNC?

The list below is for all organisations that have full access to PNC. Full access, means they can read and update records, although within each organisation the PNC Administrator will set up individual user access suited to specific roles and the type of transactions the person in that role will be required to make.

Avon & Somerset
Bedfordshire
Cambridgeshire
Cheshire
City of London
Cleveland
Cumbria
Derbyshire
Devon & Cornwall
Dorset
Durham
Dyfed-Powys
Essex
Gloucestershire
Greater Manchester
Gwent
Hampshire
Hertfordshire
Humberside
Kent
Lancashire
Leicestershire
Lincolnshire
Merseyside
Metropolitan
Norfolk
North Wales
North Yorkshire
Northamptonshire
Northumbria

Nottinghamshire
South Wales
South Yorkshire
Staffordshire
Suffolk
Surrey
Sussex
Thames Valley
Warwickshire
West Mercia
West Midlands
West Yorkshire
Wiltshire
Central Scotland
Dumfries & Galloway
Fife
Grampian
Lothian & Borders
Northern
Scottish Crime, Drug and Enforcement Agency
Scottish Government Health Directorate
Scottish Police Service Authority
Strathclyde
Tayside
Guernsey Police
Isle of Man Police
Police Service of Northern Ireland
British Transport Police
Ministry of Defence Police and Guarding Agency
States of Jersey Police
Serious Organised Crime Agency (SOCA)
Serious Organised Crime Agency (SOCA) Interpol
Service Police Crime Bureau (Army Provost RMP)
ACPO Criminal Records Office/UKCA ECR
Mersey Tunnels Police

Appendix 4A contains the PNC Service Level matrix which provides details of the organisations that can access PNC and includes the authorised level of access / transactions available. It is divided into three sections: police

family (includes all UK police forces and law enforcement agencies), extended police family (this includes all authorised agencies with a police business focus) and authorised non-police agencies (whose access is authorised to support policing purposes).

PNC can only be used for policing purposes. The Management of Policing Information 2005 (MOPI) defines "police information" as information required for policing purposes. And the MOPI code of practice defines policing purposes as:

- protecting life and property;
- preserving order;
- preventing the commission of offences;
- bringing offenders to justice;
- any duty or responsibility of policing arising from common or statute law.

These five policing purposes provide the legal basis for the collecting, recording, evaluating, sharing and retaining police information i.e. investigation, prevention and detection of crime.

6 Which organisations have restricted access to the information held on PNC? For what purposes are they permitted to access the PNC?

The list below is for all organisations that have restricted access to PNC, that is to say they cannot access the full range of PNC transactions. In some cases there may only be authority to receive an extract of specific data items, for example stolen vehicles. Where they do have direct access to PNC, their PNC Administrator will set up individual user access and the specific commands that individual can use, which may be a subset of what the organisation has been authorised to use.

AVCIS (ACPO Vehicle Crime & Intelligence Service)

HM Inspector of Constabulary

National Identification Service

NPIA Bramshill (SCAS)

NPIA Data Quality & Integrity Team

NPIA ICTLP

NPIA NDNAD

Port of Liverpool Police

Port of Tilbury Police

UK Border Agency

UK Border Agency Immigration Group

Access NI
Children and Family Court Advisory and Support Service (Cafcass)

Carweb (AMT Data Technologies)

Charities Commission for England & Wales

Criminal Cases Review Commission

Criminal Records Bureau

Driver Vehicle Licensing Agency (DVLA)

Defence Vetting Agency

Department for Business, Innovation and Skills

Department for Work and Pensions (ex DSS)

Disclosure Scotland

Environment Agency
Experian (also third party service provider of insurance information)

Financial Services Authority

Foreign and Commonwealth Office

Gangmasters Licensing Authority

Health & Safety Executive

Highways Agency

HM Prison Service

HM Revenue & Customs

HPI

Independent Police Complaints Commission

Independent Safeguarding Authority

Jersey Customs & Immigration

Ministry of Justice - Justice Statistics Analysis Service

Ministry of Justice (Jury Vetting)

Ministry of Justice - Mental Health Casework Directorate

Ministry of Justice (Warrant Enforcement)

Ministry of Justice (Bichard7)

National Air Traffic Services Ltd. (NATS Ltd)
National Health Service (Counter Fraud Operational Services)

Office for Nuclear Regulation

Office of Fair Trading

Project Semaphore - E-borders

RetainaGroup

Royal Mail Corporate Security

Scottish Society for the Prevention of Cruelty to Animals

Serious Fraud Office

The Civil Nuclear Constabulary (UKAEAC)

The Gun Trade Association

Trading Standards - Bristol City Council

Vehicle and Operator Services Agency

Vehicle Information Services (CDL)

Appendix 4A contains the PNC Service Level matrix which provides details of the organisations that can access PNC and includes the level of access. It is divided into three sections: police family (includes all UK police forces), extended police family (this includes all authorised agencies with a police business focus) and authorised non police agencies (those that support policing purposes).

PNC can only be used for policing purposes. The Management of Policing Information 2005 (MOPI) defines "police information" as information required for policing purposes. And the MOPI code of practice defines policing purposes as:

- protecting life and property;
- preserving order;
- preventing the commission of offences;
- bringing offenders to justice;
- any duty or responsibility of policing arising from common or statute law.

These five policing purposes provide the legal basis for the collecting, recording, evaluating, sharing and retaining police information i.e. investigation, prevention and detection of crime.

7. How do the organisations referred to in questions (5) and (6) above access the PNC?

By direct computer access via a nationally accredited secure network that complies with the approved network protocol. All PNC users or authorised agencies are allocated an access level that is determined by role requirement, i.e. there may only be a need to make enquiries and no need to have update access.

Alternatively other agencies such as the disclosure agencies, CRB etc receive a data download and regular updates via a secure network.

8. Which organisations are entitled to request information from the PNC and for what purposes? By what process do such organisations obtain information from the PNC?

Appendix 4A contains the PNC Service Level matrix which provides details of the organisations that can access PNC and includes the level of access. Police Forces sometimes have their own local sharing agreements, for example with the local probation service. These arrangements are matters for the Chief Constable.

Access to PNC by other organisations in their own right can be granted by the PNC Information Access Panel (PIAP), chaired by ACC David Pryde of Hampshire. The panel comprises a cross-section of expertise from different forces who meet to consider each written application for access to PNC. The process is that the business case (the organisation applying for access) must explain what is sought and why it is required. This can be a new application or any change to an existing approved requirement. The PIAP decision process is reliant on a robust business case that clearly provides a policing purpose, using the MOPI criteria. I have already listed this in my answer questions 5 and 6. The business justification must therefore assist police in the prevention and detection of crime, apprehension and prosecution of offenders.

Once an application is agreed the requesting organisation is then visited as part of a security audit. Providing there are no areas of concern, actions are taken at PNC to grant access by authorised users to the transactions and data on PNC that PIAP have authorised. Part of this process requires acceptance and signing of the relevant documentation, which includes the Supply Agreement (Appendix 8A) and Code of Connection (Appendix 8B).

9. What systems and/or measures are in place to ensure that the information held on PNC is not misused? The inquiry is interested in both technical and non-technical measures.

PNC has built in technical security measures including:

- user password control;
- access control groups built by PNCS on behalf of police forces and authorised Agencies;
- system timeout – for individual transactions;
- user access is automatically taken away following a 6 month period of the user's account being inactive;
- user accounts for anyone whose access should be removed is done so immediately upon notification;

- logins get locked-out after a 3 unsuccessful attempts and must be reset by the organisation's administrator;
- use of the CJX Restricted Network to host communications between organisations and the PNC.

When it comes to keeping information protected and secure, often known as "Information Assurance", the PNC and all of the other information systems referred to in this document, including the technical infrastructure on which they are mounted are all nationally accredited. PNC is compliant with the ACPO/ACPOS Community Security Policy (CSP), included at Appendix 9D.

Accreditation is the formal assessment that the identification and management of risks to information assets has been done to a level that the business can accept. The key principle is to ensure that the risk is being properly managed. The aim of accreditation in the police service is to maintain the confidentiality, integrity and availability of policing data to the levels required by the business. It is based on evidenced management of risk through pragmatic, appropriate and cost effective controls. ACPO Council has mandated accreditation for all operational policing information systems.

Non-technical measures include:

- Auditing to verify that a given users actions are justified by the business need. This is explained fully in the ACPO Data Protection Manual. Part 2 determines the level of audit required for PNC. All forces and those agencies identified as extended police family have a data protection function that is responsible, on behalf of chief constables, to audit PNC data (Please see Appendix 9A).
- Audit of non-police agencies has been undertaken by NPIA on a 3 year rolling schedule basis. This has been both physical security and to ensure that an audit function is in place in the organisation and is operating correctly.
- Any reported instances of non-compliance are investigated immediately and followed up by either corrective action or ultimately access can be removed.
- Training – the national standard requires all users of PNC to attend an approved training course. Course objectives include communicating what the system can be used for, warnings against misuse, what constitutes misuse and the consequences of such action. An example is included at Appendix 9B.

Forces also have their own audit plans and these often work in conjunction with other police departments such as Professional Standards etc. Hertfordshire Constabulary and Essex Police, by kind permission,

have provided their PNC audit plans to me as examples and are included at Appendix 9Ci-iv.

10. Are individual users subject to any vetting procedures or security checks? If so, please give details. Is there a system in place for monitoring and reviewing the suitability of a person to have continued access to the PNC? If so, please give details. Who is responsible for carrying out such checks/reviews?

Vetting of police officers and staff is a matter for chief officers. To my knowledge the vetting of police officers and police staff is governed by the ACPO/ACPOS National Vetting Policy for the Police Community (Appendix 10A) and the NPIA Circular 01/2010 (Appendix 10B), which was driven by the HMIC report "Raising the Standards" (Appendix 10C). These documents clearly outline the requirement for standards and frequency of vetting.

NPIA PNC Services staff must achieve the national vetting standard of SC clearance before they commence work at the site, and only those few who need to work on live systems are granted access. All access to live systems is recorded and 100% audited on a monthly basis by my systems security team. In addition, where possible, work is divided so that more than one person is involved in any given task as a deliberate strategy to limit risk.

Security clearances for NPIA staff are reviewed on a rolling basis of between five and ten years. Should the few individuals who have access to PNC, fail these checks they would have their access to the system removed, where appropriate.

11. Are any restrictions placed on an individual PNC user's ability to access information held on the PNC (whether by technical means or by way of instructions to the user)? For instance, are users permitted to browse the database without restriction?

Under Question 13 further on in this document I have described a system within PNC that carries out comprehensive logging of all transactions carried out on the PNC. These logs record all user activity on the system to the extent that both what was requested and the resulting response to the request by PNC can be interrogated. In the case of requests, this is date and time stamped and held on the Transaction Log (Tlog). In the case of the information sent back, the Message Log (Mlog), provides exactly what was viewed. Interrogation of Tlogs can be carried out on-line by the authorised user. Mlogs are run at the data centre, as a batch job,

upon receipt of a written request from a force's authorised signatory. In the case of an Mlog for over 12 months activity the request must also be signed by an ACPO rank.

The PNC system requires the user to complete a number of specific data items before it will carry out any enquiry. These include who you are and why you are carrying out the specific check. This shows up in the log and again can be audited against.

The overt logging of transactions not only provides a record of what is being asked and the response but also acts as a deterrent to unlawful access because it is available for subsequent analysis and is accepted and used in court as part of the evidential record.

Under the Government Protective Marking Scheme (GPMS) PNC is classified as "Restricted", and therefore its contents must be treated in accordance with that scheme. To my knowledge, most if not all forces make this clear on their system splash screens, the entry screen. For example, by using data protection warning signs like "only authorised users may proceed".

Access by any organisation is in accordance with business need. Access can be limited not only to read, but also controlled by the individual types of transaction that are made available. For example – names only, vehicles only, vehicles and property only.

A particular group of users, within an organisation, can have controls placed on the transactions that they can use, or indeed a particular user can be empowered or restricted. These are centrally controlled by my staff at Hendon Data Centre.

In addition an organisation's own administrator(s) can decide who in that organisation gets access, which again can either be access to all of the transactions granted to that organisation or limited to a sub-set.

Examples of different organisations being granted different levels of access can be clearly seen within the Service Level Matrix at Appendix 4A.

PNC users are required to be trained to a national standard, a standard of PNC Training documentation that is signed off by the ACPO lead. Of course the responsibility for ensuring this happens is down to the organisation.

The fact that some Police Officers and Staff are convicted and/or disciplined for data misuse in relation to PNC and other systems is evidence that firstly safeguards do identify some inappropriate or illegal

use, secondly the Police Service does take action and thirdly, the fact that some of this is made public, means deterrents are in place.

12. What training is provided to individual PNC users to ensure that they understand what is and what is not lawful/appropriate use of the information held on PNC? Who is responsible for providing the training?

All NPIA PNC courses are accredited to an ACPO approved standard. PNC Training Standards are progressed by the Training Working Group (TWG) making recommendations to ACPO for approval. The quality of PNC training was the subject of a 2005 HMIC Inspection Report PNC Training Matters, see Appendix 12D, emphasised the importance of this training and the national standards.

All PNC Trainers are accredited by attaining the national standard and have to complete an annual registration. NPIA National PNC Accreditation Process is included at Appendix 12A. The national PNC trainers register is held centrally by NPIA.

The NPIA provide a series of nationally approved courses for different PNC levels that adhere to a set of national aims and objectives. To enable understanding of what is and what is not lawful/appropriate use of PNC data, relevant aims and objectives relating to Information Security are built into all PNC courses. Appendix 12B provides an example of a PNC Names Enquiry course's aims & objectives please see objectives 3-6.

Police forces and a small number of other organisations provide PNC training. The PNC Manual (Appendix 4C) forms the basis of the training and is electronically available and a pocket guide, known as the "Blue Book", assists all users with basic knowledge. Please see Appendix 12C, for the booklets contents and specifically page 7 for a reminder / warning of Data Protection and Computer Misuse Acts.

Chief Constables are ultimately responsible for ensuring their Police Officers and staff work and behave in accordance with ACPO standards. This includes the use of PNC and ensuring that they use the systems as intended and that auditing takes place.

13. What systems and/or measures are in place to audit the use of the PNC by individual users? Describe the system of auditing, if any, that is in place, who is responsible for this auditing process?

All transactions on PNC are recorded, first by Transaction Log (TLOG) and the responses provided are recorded on Message Log (MLOG). Both logs are retained for 18 months and can be searched for different types of activity. (For example, who stopped this vehicle or what information a user viewed when accessing PNC). Each force's professional standards staff would follow up any concerns of unauthorised access or misuse of PNC information. Other Agencies can also make use of this facility in respect of their own staff (e.g. SOCA).

PNC also provides certain services to the Police where they submit a job request to Hendon Data Centre and these queries / jobs are typically run overnight. The results, in the form of images of prints or data extracts are sent, normally electronically to the authorised requesting agency. These jobs must be requested by authorised signatories who are registered with PNC and which are themselves subject to regular review.

Details of the audit requirements for users are included in the Data ACPO Protection Manual, which can be found at Appendix 9A. Forces undertake their own audits, an example of which is shown at Appendix 9C, and are responsible for taking appropriate action on the outcomes.

HMIC inspect forces for compliance against the Code of Practice.

14. What systems and/or measures are in place (i) to prevent; (ii) detect and (iii) to deter individual PNC users from unlawfully disclosing information?

Although I have a broad overview of this area, other than the measures mentioned above, such as PNC policy, training, system security and audit, this is beyond my area of expertise and responsibility. This is a matter for forces and other authorised organisations with access to the PNC.

15. Do you consider that the systems and/or measures referred to in questions (12) above work effectively? What changes, if any, do you consider should be made to them?

Yes. The standards and framework are in place. Obviously they must be utilised and auditing must take place. I believe that knowledge and understanding does however need to be refreshed periodically. Within the

Agency our Information Assurance knowledge is tested on an annual basis and the pass level must be met or exceeded. Perhaps such an approach, which may already be in place in some forces, would help.

With the phasing out of NPIA at the end of 2012, it is currently being determined where PNC training should sit and how national PNC training standards will be maintained and where appropriate, improved upon.

16. Were changes made to any policies or procedures or systems relating to use of the PNC and the security of the same following Operation Motorman, Glade and Reproof? If so, please specify.

I am unable to answer this question for two reasons. I was not in post at this time and therefore have no personal knowledge of any system changes. I have also looked for references within the change control system that records all system changes to PNC that have been made or are awaiting implementation but none were identified that referred to these operations.

Should any reference or other evidence be found that links any changes to PNC these will be made known to Lord Justice Leveson.

It may be that those who ran or oversaw those operations are better placed to answer this.

17. In the last 5 years, how many investigations have there been into suspected unlawful disclosures of information held on PNC to the media and/or private detectives? What was the outcome of those investigations? Who is responsible for conducting such investigations? Insofar as the suspects were police officers or civilian police staff, please provide a breakdown of how many were serving with the MPS and how many were serving with other police forces.

I have no knowledge of either the number of investigations or the outcomes other than what I have seen in the media. My staff fully support forces in running enquiries against the two types of log files that we hold, (described to you in my answer to your Question 13).

Each Force is, in the first instance, responsible for conducting such investigations.

I am not aware of any centrally held information as to the number of investigations or the outcomes and believe that each force / organisation would have to be asked to supply this.

Included below are the number of searches that we were asked to carry out at the Hendon Data Centre in the calendar years 2010 and 2011. A search could be for a period up to 15 months for Message Log (Mlog) or up to 12 months for the Transaction Log (Tlog). Examples of a search include a name, an address, a vehicle, an operator, updating or reading records. In the case of the Transaction Log it will return all matching search or update records, and in addition for Message Log it will show the screens of data and the content that PNC provided.

Totals for 2010	**1,404**
Tlogs	**1,008**
Mlogs	**396**
Totals for 2011	**1,431**
Tlogs	**1,157**
Mlogs	**274**

The Transaction Log figures do include a regular monthly run of all activity for 44 of the Police Forces, which accounts for 44 x 12 = 528 runs per calendar year. (Transaction Log searches can also be carried out on-line by forces. The total number of on-line TLogs for 2010 was 1,195,075 and for 2011 was 1,118,161).

Forces are known to use these logs for a variety of different purposes, not just for their investigations of PNC misuse.

I would respectfully direct you in the first instance to ACC David Pryde of Hampshire Police for more information or the ACPO lead for Professional Standards.

18. Do you consider that the unlawful disclosure of information from the PNC is a current problem? Please explain your answer.

There is, without doubt, evidence that the PNC is misused occasionally and that misuse, from time to time, involves unlawful disclosure. It is for that reason that safeguards are in place both at a national and an individual force level. It is our aspiration that the system will never be misused, but that is quite possibly unrealistic. We believe that the current security measures are effective and proportionate and that, although no unlawful disclosure is acceptable, I do not think that there is a widespread

systemic problem, nor that any particular and specific additional security measure would be effective.

19. What additional measures, if any, should be put in place to prevent the unlawful disclosure of information held on the PNC?

PNC is a system that is widely used, playing a vital part in supporting operational police officers and other police staff. At the time of use, these staff mainly need information very quickly or indeed to load some information onto PNC quickly, for example to get a vehicle stopped, share information that a person is wanted and is to be detained or share vital information for officer safety. This need for immediate and free access (which encourages use of the system) needs to be weighed against any additional security or safeguard.

Similarly, any increase in the extent to which data is retained needs to be considered carefully. Although improving our ability to audit, it also increases the quantum of data held centrally which has implications for privacy and human rights.

NPIA and the Police Service have introduced Identity and Access Management (IAM) which is being rolled out across a variety of systems. Identity and Access Management (IAM) is a security architecture encompassing technical, procedural and personnel security mechanisms and utilising a Public Key Infrastructure (PKI) under the control of a single governance structure that:

- enables secure sharing of police service information within the police service, with partner organisations and with the public;
- facilitates access by the police service to information held by other organisations;
- provides certificates and other support to all forms of software based cryptography within the Police Service.

IAM provides a facility to fulfil a critical business need to share information and intelligence securely whilst enabling it to be more widely available. It is already being used for the Police National Database and will next be used on our soon to be implemented CRASH project (recording of road collisions). Over time, we should push to use our IAM as a basic tool for all systems.

Beyond the more extensive use of IAM, the NPIA view is that there are no other additional measures that are capable of being implemented that would make a meaningful contribution to managing the risk in this area.

Statement of Truth

I believe the facts stated in this witness statement are true.

Signed .....

Dated: 16th March 2012

Karl Wissgott FBCS, MSc, CITP

Head of PNC Services
National Policing Improvement Agency