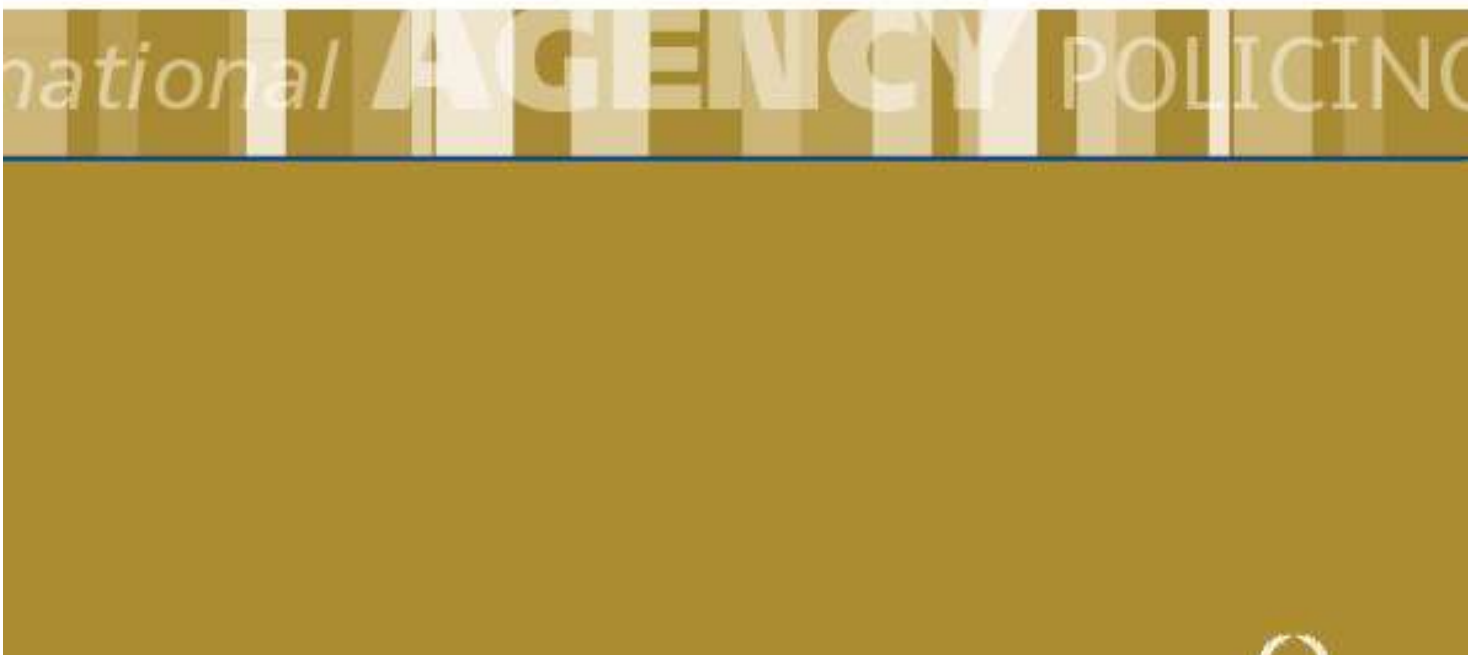
NATIONAL ACPO ANPR STANDARDS (NAAS)

Version 4.12
November 2011



Freedom of Information Act

This document NAAS is not protectively marked and is suitable for publication and should be made available for public access under the Freedom of Information Act.

Document Approval

Name	Signature	Date	Title/Organisation
Prepared by:	John Dean	Nov 2011	National ANPR Co-ordinator
Authorised by:	Simon Byrne	Nov 2011	DCC Greater Manchester Police ACPO Lead for ANPR

CONTENTS

Version Control

Author	Reason for change	Version	Date
Geoff Chandler	First update following the original release of the NAAS.	1.5	May 2003
Geoff Chandler	Update in support of National Strategy	2.6	August 2006
Geoff Chandler	Update in support of National Strategy and reflect the implementation of the NADC	3.0	May 2007
John Dean NPIA National ANPR Co-ordinator	Updated and consolidated to come into line with NPIA working practices	4.0	July 2008
Bill Mandeville	Updated to reflect ACPO-signed MoUs	4.12	November 2011

1 Introduction

1.1 To enable development and integration of Automatic Number Plate Recognition (ANPR) in the UK, it is essential that all ANPR Systems operated by the Police Service in England, Wales and Northern Ireland are compatible with one another and are compliant with a common standards supporting a national strategy. These standards are the National ACPO ANPR Standards (NAAS).

1.2 The current version of the ACPO ANPR Strategy for the Police Service – 2007 to 2010 together with NAAS (Version 3) was approved by Chief Constable's Council in October 2007. The NAAS supports the ANPR Strategy in clearly defining the minimum standards required to ensure local, regional and national ANPR objectivities can be achieved.

1.3 The revision of the NAAS to Version 4 consolidates some sections within earlier documents to provide improved clarity of the common standards required for ANPR systems. The technical standards are identical to those approved within Version 3, only the format has changed.

1.4 The original National ANPR Standards – Minimum Requirements were developed to aid the development and rollout of Project Spectrum. The Minimum Requirements were then further refined in May 2003 (Issue 1.5) and later replaced by the National ACPO ANPR Standards in March 2005 (Issue 2.6). NAAS Version 2.6 was endorsed by Chief Constable's Cabinet in October 2004.

1.5 This update of the NAAS (Version 4.12) replaces (Version 4.11). Rules around data retention and access have been updated to reflect the ACPO and ICO agreed standards. No technical standards have been changed, other than references to BOF II v2.2 have been updated to v2.3.

1.6 This document does not mandate the use of any specific product(s).

2 Minimum Requirements

2.1 ANPR Systems – General

These requirements relate to force ANPR systems including all components of infrastructure that constitute the force ANPR environment. It also includes those components that are under the ownership or control of identified partners. In particular the systems will include the Number Plate Reading Device (NRD), the Back Office Facility (BOF), communications links, firewalls and other related supporting components.

2.1.1 Time Synchronisation

The Force ANPR Environment must be fully synchronised with a Global Positioning Signal (GPS) time source. Greenwich Mean Time plus zero (GMT +0). All key component parts (in particular the BOF, NRDs, mobile ANPR systems and servers) must synchronise every 10 minutes.

2.1.2 Government Protective Marking Scheme (GPMS)

All ANPR Systems must conform to, and support, the Government Protective Marking Scheme.

2.1.3 Schengen Information Systems

All ANPR Systems must meet the requirements of Schengen II when the Schengen Information Systems come into operation. *[date to be confirmed]* and must be capable of reading plates that form part of the Schengen community including NI and ROI plates. These include:

Austria, Belgium, Bulgaria Cyprus Czech Republic Denmark, Estonia Finland, France	Germany, Greece, Hungary Iceland, Italy, Latvia Lithuania Luxembourg, Malta	Netherlands, Norway, Poland Portugal, Romania Slovak Republic Slovenia Spain Sweden

2.1.4 Police Corporate Data Model (CorDM)

All ANPR systems must be compliant with the CorDM standards prevailing at the time of installation.

2.1.5 Information Systems Strategy for the Police Service (ISS4PS)

All ANPR systems must be compliant with the ISS4PS requirements prevailing at the time of installation, Procurement and or sign-off.

2.1.6 Performance Evaluation

An annual Performance Evaluation of the all ANPR systems must be conducted to ensure minimum performance levels are maintained in line with the standards detailed in NAAS.[1]

2.1.7 ANPR Procurement

All equipment procured for connection to Force ANPR systems and the NADC must conform to the requirements of these standards.

2.1.8 Web Services

Web services specifications do not form part of the NAAS but are essential information supplemental to those standards. They describe the interfaces BOF 2 provides for connecting to other BOFs and to source equipment for the transfer of information. BOF 2 has been designed to use web services to facilitate the interconnection of other ANPR and non-ANPR systems, such as force intelligence systems (FIS) and Geographical Information Systems (GIS). Data flows and high level interfaces are portrayed in diagrams and detailed web service and Web Service Description Language (WSDL) definitions are provided.[2]

2.2 ANPR Systems – Performance Requirements

2.2.1 Static ANPR Camera Systems (Fixed Assets)

A static ANPR camera system is one that has been built for the primary purpose of 'capturing' and 'reading' VRM. The camera is located in a fixed

[1] Guidelines on the evaluation of performance are provided in the document "ANPR Performance Evaluation" Capita Symonds Ltd, 2006.
[2] Details of Web Services Specifications are provided in the document BOF 2.3 Web Services.

position. Performance standards for Static ANPR camera systems must be achieved at all times (24/7).

2.2.2 CCTV Integrated ANPR Systems

A CCTV Integrated ANPR (Dual purpose CCTV and ANPR Camera which are connected to the matrix) system is one that has been built for the primary purpose of CCTV monitoring but has ANPR added to the system for the purpose of 'capturing' and 'reading' VRM. The camera should be optimised for the purposes of ANPR. Performance standards for dual purpose CCTV and ANPR cameras within integrated systems must be achieved at all times when deployed in ANPR mode (24/7). The CCTV matrix must provide detail of the outputs of the camera; Monitor and macro to enable the camera location to be accurately displayed.

The readers attached in ANPR mode must only attempt to provide data where the correct camera and macro details are being supplied.

2.2.3 Mobile ANPR Camera Systems

A mobile ANPR camera system is one that has been built for the primary purpose of 'capturing' and 'reading' VRM. These include Vehicle Mounted ANPR systems, Laptop or other portable based ANPR systems and Air Support Mounted ANPR systems. To achieve the optimum performance requirements mobile equipment should be capable of night time and low light operation. There are performance considerations to be accounted for in relation to mobile equipment when it is being deployed in motion or when stationary.

2.2.4 'Capture' and 'Read' rates for All United Kingdom (UK) and Schengen Community Number Plates

ANPR systems must achieve as a minimum the following levels of performance in 'capturing' and 'reading' VRM in comparison with the total number of vehicles passing through the ANPR camera for all legitimate UK and Schengen Community number plates.

Type of System	Capture Rate	Correct Read Rate	Overall capture & correct read rate
Static ANPR Camera	98%	95%	93.1%
CCTV Integrated ANPR (Dual purpose CCTV and ANPR Camera)	85%	85%	72%
Mobile ANPR Camera (Stationary)	98%	95%	93.1%
Mobile ANPR Camera (Moving)	80%	85%	68%

2.2.5 'Capture' and 'Read' rates for All Schengen Community in Isolation of United Kingdom (UK) Number Plates

ANPR systems must achieve as a minimum the following levels of performance in 'capturing' and 'reading' VRM in comparison with the total number of vehicles passing through the ANPR camera for all legitimate UK and Schengen Community number plates.

Type of System	Capture Rate	Correct Read Rate	Overall capture & correct read rate
Static ANPR Camera	85%	80%	68%
CCTV Integrated ANPR (Dual purpose CCTV and ANPR Camera)	85%	80%	68%
Mobile ANPR Camera (Stationary)	85%	80%	68%
Mobile ANPR Camera (moving)	75%	80%	60%

The circumstances under which an evaluation of Schengen Community plate reading capability should be undertaken in isolation are:

Where the ANPR system is installed at a port
Where 10% or more of vehicle sightings relate to non UK plates.

[for avoidance of doubt UK includes Northern Ireland, Isle Of Man, and Channel Islands number plates]

2.2.6 Data Output from ANPR Systems to BOF

All ANPR Systems must provide an output to the BOF the minimum ANPR data for each 'read' as detailed below:
VRM
Date and Time of 'read' to the nearest second (GMT +0)
Camera, Feed (Force ID) and Source (Scarab ID) Identification
GPS Coordinate for the location of the 'read' accurate to within 5 metres
Plate patch image (JPEG)

And may also include:

Confidence Level in the accuracy of the 'read'
CCTV Preset Value (for CCTV ANPR systems)
Overview Image (in JPEG format)

Where included, the overview image should allow for:

Identification of the Make, Model and Colour of the vehicle
Identification of the vehicle in the context of the 'capture' zone
A maximum image size of 25 Kbytes.

NB. When a mobile ANPR unit is unable to deliver an accurate GPS coordinate for a read, the GPS field must be populated with a zero figure, presented in a valid GPS coordinate format. For example: (N0000000 E00000000) ANPR reads must not be output with the GPS field left blank or populated with the last known coordinate.

2.2.7 Plate Patch Image

Where plate patch images are sent to the BOF separately to ANPR 'read' data the image must be able to be linked to the 'read' data to which it relates.

The plate patch must meet the following standards:

A be of a minimum size of 120 pixels x 60 pixels
B be such that the index plate shall be identifiable when displayed on a 1024 x 768 pixel screen with the index plate occupying no more than 60 pixels in height.
C have a maximum size of 3Kbytes.

Output data size

The following standards are required for a 1024 x 768 screen

	Maximum size in KB	Minimum pixel	Maximum height in pixel
Text	0.8		
Plate Patch	3	120 x60	60
Overview Image	25		

2.2.8 ANPR Systems – 'buffer' storage capacity

All ANPR systems must have the capacity to store ANPR 'reads' and their related images for a minimum period in a cyclical buffer of 48 hours should the BOF or communications to the BOF become unavailable.

2.2.9 Transfer of 'Read' data from Mobile ANPR Systems to BOF

All ANPR read data held on mobile ANPR units that have been unable to transmit their data to the force BOF shall be transferred onto the BOF within a maximum period of 48 hours from the time of capture.

2.2.10 ANPR System Resilience

All ANPR systems must have a mean time between failures of the system of not less than 5,000 hours and a minimum availability of 99.9% or greater.

2.3 Back Office Facility (BOF)

The BOF must enable compliance with the following:

2.3.1 Centralised management of ALL ANPR 'reads', ANPR 'hits' and ANPR 'hotlist' data within each force.

A single repository (or integrated repository) will allow for easier management of ANPR data and maximise access to that data in an efficient and secure manner. The data need not be managed in a single location. It is desirable to maintain the Force ANPR data in locations to

provide both a Primary System and a Backup or Disaster Recovery System.

Forces may choose to store ANPR data on one hardware environment with related images stored on a separate hardware environment optimised for the storage of images. Forces should not operate multiple BOF that contain ANPR data from different sources, managed separately.

2.3.2 BOF connectivity to force networks and to CJX (PNN2/PNN3).

The Force BOF must connect to the Force network infrastructure and CJX to allow user access to the BOF and facilitate access to the CJX via the Force Secure External Gateway, to support connections to the Police National Computer (PNC), the National ANPR Data Centre (NADC) and other BOF.

The Security of all connections to the BOF must be managed via a Force maintained and managed firewall in accordance with the Forces own policy and the CJX Code of Connection and Security Policy.

2.3.3 National Hotlists

The BOF shall have the capacity to run the following national hotlists as a minimum.

PNC Extract File
Driver and Vehicle Licensing Agency (DVLA) (No Current keeper and No VEL)
Motor Insurance Database (MIDAS)

The BOF **MUST NOT** synchronise the above national hotlists with the NADC.

2.3.4 Real-time matching against PNC (#RE Fast Track) and other 'Hotlists' for ALL ANPR 'reads'.

The system response time from a Vehicle Registration Mark (VRM) being captured by a Number Plate Reading Device (NRD) to the hit notification response being delivered to a specific operator must not exceed **4 seconds** for Static ANPR systems and all CCTV ANPR Integrated systems and **6 seconds** for Mobile ANPR systems.

To allow for this end-to-end performance requirement, the NRD must deliver ANPR reads to the BOF within **2 seconds** of capture for Static ANPR systems and all CCTV ANPR Integrated systems and within **4 seconds** of capture for Mobile ANPR systems.

The BOF must process that read against the PNC and other hotlist databases and deliver any resultant match notification to the operator within **2 seconds** of receipt of the read by the BOF for all systems.

The PNC Extract File is provided to forces at least once every 24 hours and must be loaded onto the BOF upon receipt. All ANPR reads must match against the PNC Extract File should the live link to the PNC be unavailable.

Maximum time (seconds)

System Type	Read to alarm	Number plate capture to delivery to BOF	BOF process to delivery
Static Reader	4	2	2
CCTV Linked reader	4	2	2
Mobile system	6	4	2

2.3.5 Real-time delivery of data to the National ANPR Data Centre (NADC).

The BOF must deliver data to the NADC within **10 seconds** of capture by a NRD.

In the event of a communications or systems failure, the BOF must buffer all data, and deliver that read data to the NADC, once the communications or failed systems have been restored.

The Force BOF must support the following means of data communications with source systems in order to meet data delivery standards:

Local – TCP/IP over the Force network

Regional – wireless transmission (GSM, GPRS, 3.XG and 802.x from a remote mobile device)

National – CJX from Forces, PNC and the national ANPR systems.

Data transmission mechanisms must be afforded security measures that accord with GPMS.

2.3.6 Interoperability between other force BOFs and NADC

Force systems must enable interoperability between other force BOFs and NADC to allow:

a. Hotlist distribution to other force BOFs and NADC.

b. Real-time matching of reads against hotlists and the real-time delivery of hits.

c. Remote BOF research in accordance with prevailing researching guidelines .

d. NADC read searching for national data searches and data mining in accordance with the NADC / BOF Business Rules, as defined within current Memoranda of Understanding (MOU) for access to NADC and other databases (BOF to BOF).

2.3.7 Security of the BOF and all data communications.

The BOF must provide adequate security measures, including access control, to protect against unauthorised access to the system and data held within it. Individual user privileges must require a minimum of CTC security clearance.

Audit trails must be maintained to record all significant actions taken such as user login, database searches, adding and deleting data from hotlists and access to audit trails must be restricted to users whom require this access as part of their role.

The Security of all connections to the BOF must be managed via a Force maintained and managed firewall in accordance with the Forces own policy and the CJX Code of Connection and Security Policy.

All communications to and from the BOF must be encrypted to a minimum strength 128bit except where the communications is across a RESTRICTED network. However it is desirable that these communications are also encrypted.

The BOF server must be protected from Not Protectively Marked (NPM) networks by a Communications-Electronics Security Group (CESG)

approved, E3/EAL4 accredited firewall to protect access to the system from unauthorised external connections

This requirement applies to all communication with the BOF including source ANPR systems, other force BOF and NADC.

The BOF must support compliance with the requirements of the Government Protective Marking Scheme (GPMS).

3 Hotlists

The PNC Extract File is provided to forces at least once every 24 hours and must be loaded onto the BOF upon receipt. All ANPR reads must match against the PNC Extract File should the live link to the PNC be unavailable.

Where data is provided by a 3rd party (e.g. the PNC Extract File as provided directly/indirectly from PNC) then the force must implement measures/procedures to ensure that the data is handled in an appropriate manner. The criteria that must be addressed through these procedures include:

a. Secure and auditable onward distribution to any third party (individual and/or system)
b. Guarantee currency of the data set (i.e. is the most up-to-date file in use)
c. Version control and file naming
d. Means of distribution satisfies GPMS security requirements
e. data must not be issued to `non-Police' personnel unless specifically authorised by an ACPO ranking officer within force.

All hotlists maintained by a force at a local level must comply with the following standards:

3.1 Hotlist Template

All hotlists must conform to the national hotlist template.

Column	Description	Standard Words	Comment
1	VRM		No Spaces
2	MAKE		
3	MODEL		
4	COLOUR		
5	ACTION 1ST WORD	Stop Silent Intel	 Silent sightings only. Do not stop for routine checks. If additional grounds exist vehicle may be stopped

		DO NOT STOP	For reasons of officer safety or investigation requirements
6	WARNING MARKERS 2nd WORD	Nothing Known (NK) Firearms (FI) Weapons (WE) Violent (VI) Fails to Stop (FT)	Enter maximum of 3 relevant markers
7	REASON 3rd WORD	Drugs Crime Disqualified Docs Drink Drive Sexual Other Protest VISOR NO STOP Intel	For 'silent checks' enter NO STOP
8	INTEL 5X5X5		Enter grading without X or spaces
9	INFORMATION/ ACTION	Prefix free text with date and time in format [dd/mm/yyyy hh:mm]	Brief free text to include and additional information and Force reference number if applicable
10	FORCE AND AREA		Include Force Name/ Area (BCU/Division letter) and 24hr contact tel no.
11	WEED DATE		
12	PNC I.D.	1 Firearms 2 Explosives 3 Fails to stop for Police 4 Weapons 5 Violent 6 Suicidal 7 Mental 8 Escaper 9 Drugs 10 Contagious 11 Alleges 12 Ailment 13 Offends against Vulnerable Person 14 Sex Offender 15 Female Impersonator 16 Male Impersonator	
13	GPMS marking		Restricted
14	CAD		
15	SPARE		
16	SPARE		

4 Data Retention and Access Control

4.1 Record retention and Deletion

ACPO guidelines specified in conjunction with the Information Commissioners Office (ICO) state that capture records must be deleted no later than two years after their initial capture. The only exception to this rule is when, requirements arising from consideration of the Criminal Procedure and Investigations Act (CIPA) 1996, alternative retention periods are appropriate.

4.2 Provisions for access to ANPR data held on local force databases must be detailed within force policy taking account of the requirements of legislation. PNC/DVLA and ANPR 'Read' data is 'Personal Information' as defined by the Data Protection Act and force policy for access to other ANPR databases must be consistent with the following:

4.2.1 **Access to other force Databases (BOF to BOF)**

The terms of agreed MOU require that the ANPR Chief Officer lead within an organisation will designate a member of staff of at least Superintendent rank or equivalent who is accountable for the authorisation of staff who may access another organisation's ANPR systems for investigation or intelligence purposes. Authorised members of staff will be in dedicated investigation or intelligence roles and limited to a small number of people proportionate to the extent that access is required.

Age of Data	Purpose	Authorisation Required
'Real Time'	When monitoring alarms from a NRD for Operational Response purposes.	Any member of staff authorised to access ANPR systems with no additional authority required.
Up to 90 Days	Counter Terrorism Investigations Major Investigations Serious and Complex Investigations [Appendix A] Volume and Priority Investigations	Any member of staff authorised to access ANPR systems owned by other organisations with no additional authority required.

91 Days to 1 year	Counter Terrorism Investigations Major Investigations Serious and Complex Investigations [Appendix A]	Any member of staff authorised to access ANPR systems owned by other organisations with written authority of an Inspector or equivalent staff grade.
1 year and over	Counter Terrorism Investigations	Any member of staff authorised to access ANPR systems owned by other organisations with written authority of Superintendent or equivalent staff grade.

4.2.2 **Access to NADC**

The terms of agreed MOU require that The ANPR Chief Officer lead within an organisation will designate a member of staff of at least Superintendent rank or equivalent who is accountable for the authorisation of staff who may access another organisation's ANPR systems for investigation or intelligence purposes. Authorised members of staff will be in dedicated investigation or intelligence roles and limited to a small number of people proportionate to the extent that access is required.

Age of Data	Purpose	Authorisation Required
Up to 90 Days	Counter Terrorism Investigations Major Investigations Serious and Complex Investigations [Appendix A]	Any member of staff authorised to access the NADC for enquiries that have the written authority of an Inspector or equivalent staff grade.
91 Days to 1 year	Counter Terrorism Investigations Major Investigations Serious and Complex Investigations [Appendix A]	Any member of staff authorised to access the NADC for enquiries that have the written authority of Superintendent or equivalent staff grade.
1 year and over	Counter Terrorism Investigations	Any member of staff authorised to access the NADC for enquiries that have the written authority of Superintendent or equivalent staff grade.

Glossary of Terms, Abbreviations and Definitions

ACPO	Association of Chief Police Officers (England and Wales)
ACPOS	Association of Chief Police Officers (Scotland)
ANPR	Automatic Number Plate Recognition
ANPR Systems	Includes all aspects of an ANPR such as cameras and Back Office Facility
APS	Anite Public Sector
BOF	Back Office Facility
Capture	Process by which a VRM is read
CCTV	Closed Circuit Television
CESG	Communications-Electronics Security Group
CJX	Criminal Justice Extranet
CT	Counter Terrorism
DPA	Data Protection Act
DVLA	Driver and Vehicle Licensing Agency
ECHRA	European Convention on Human Rights
FastTrack	Real time matching against PNC (#RE transaction)
File Extract Server	Server used to hold and distribute the current PNC Extract File and WCP File. (To be replaced under current NADC programme of works)
FIS	Force Intelligence Systems
FIXED ANPR	Includes all ANPR readers that form a permanent installation
FOIA	Freedom of Information Act
GIS	Geographical Information Systems
GPS	Global Positioning System
GPMS	Government Protective Marking Scheme
Hotlist	A Hotlist is a database of vehicle registration marks (VRM) of special interest. If a match occurs between a VRM on a Hotlist and a captured index delivered to either the BOF or NADC then the appropriate users shall be notified. **Local:** Includes all Hotlists that are locally created and exclude National Hotlists **National:** Includes PNC, DVLA (NCK & NVEL) MIDAS, Merged DVLA & MIDAS
ISDN	Integrated Services Digital Network
ISS4PS	Information Systems Strategy for the Police Service
JPEG	Joint Photographic Expert Group. This is a compression algorithm enabling images to be compressed and hence transmitted more efficiently.
MIDAS	**M**otor **I**nsurance **D**atabase and **A**NPR **S**ystems

MOBILE ANPR	Includes all ANPR readers that are installed in a vehicle
NAAS	National ACPO ANPR Standards
NADC	National ANPR Data Centre
NI	Northern Ireland
NRD	Number plate Reading Device
PNC	Police National Computer
PNC EXTRACT FILE	File containing a snap-shot of those Vehicle Records held on the live PNC Vehicles Database
PORTABLE ANPR	Includes all ANPR readers that are not permanent installations and could include ANPR fitted in vehicles
ROI	Republic of Ireland
Scarab	Home Office free issued software to all England & Wales Forces to link 3rd party ANPR devices to BOF
Schengen	The Schengen information system will enable the authorities of signatory countries to have access to reports on persons and objects for the purpose of border checks and controls and other police and customs checks.
Spectrum	Project Spectrum as delivered under a PITO framework contract
STATIC ANPR	Will include all permanent ANPR reader installations as well as Portable and Mobile ANPR reader when they are static
VRM	Vehicle Registration Mark
WCP	West Coast Ports file
#RE	Real time [Fast Track] PNC transaction for ANPR
#VE	PNC transaction code for manual enquiries and a limited number of ANPR systems
#VK	PNC transaction code for manual enquiries and a limited number of ANPR systems
WSDL	Web Services Description Language

APPENDIX A

Investigation Categories

Investigations within the Police Service fall within three main categories, so that there is a consistency of understanding within the service as to which investigations should be included within each category. The main categories are:

- Major Investigations
- Serious and Complex Investigations
- Priority and Volume Investigations

A consideration of the category of the investigation informs effective management and decision making, including the scope for an investigation and determination of the resources that are to be deployed. These categories provide the framework to support a National policy for retention of, and access to ANPR data.

Designated Major Investigation Categories

A key characteristic is that Major Investigations should be led by a Nationally Registered Senior Investigating Officer (SIO)

Table 1

Murder
Attempted Murder
Threat to Murder
Manslaughter
Infanticide
Child Destruction
Kidnapping
Terrorist related crimes

Designated Serious and Complex Investigations

Table 2

Arson
Abduction
Aggravated Burglary dwelling and non dwelling
Arson High Value or life endangered
Blackmail
Drug Trafficking
Death by Dangerous Driving
Fraud and Associated Offences (80hrs + investigation time)
Gross Indecency Child
Perverting Justice
Public order (racially motivated)
Rape
Robbery (F/Arms or ABH injury)
Sexual Assault (children under 13)
Wounding (S18/20)

Serious and Complex Investigations may, with the authority of a Superintendent, be escalated to the category of Major Investigations. Any authority to escalate to the higher category together with the reasons for the grant of that authority must be recorded and will take account of the following factors:

Table 3

Consideration	**Examples**
Community factors	• Likely to escalate into large scale disorder or critical incident • Has escalated from a previous offence • Sensitivity regarding individuals involved
Offence characteristics	• Aggravating factors of the offence • Vulnerability of victims/witnesses, • Has crossed force or national boundaries • Forms a previously undetected series
Offender Characteristics	• Organised crime • Terrorism links • Resistance to police operational strategies • Multiple offenders

Priority and Volume Investigations

Investigations not included within the above categories will be considered as within the remit of Priority and Volume Investigations. In particular, this will include investigations into street robbery, burglary and vehicle-related criminality and non-crime issues such as anti-social behaviour.

Priority and Volume Investigations may with the authority of an Inspector be escalated to the category of Serious and Complex Investigations. Any authority to escalate to the higher category together with the reasons for the grant of that authority must be recorded and will take account of the following factors:

Table 4

Consideration	**Examples**
Community	• High risk of critical incident • Sensitivity regarding individuals involved

Offence Characteristics	• Aggravating factors of the offence such as:
	  • Hate crime
	  • Weapons used
	  • Injuries sustained
	  • Vulnerability of victims/witnesses,
	• Priority issue identified within NIM business process.
	• Series of offences e.g. forensic links to the offender(s)

Offender Characteristics	• Criminal history • Resistance to police investigative strategies • Prolific offender - TICs • Multiple offenders