National ANPR Standards for Policing

Part 2 – ANPR Infrastructure Standards

Version 1
May 2013

CONTENTS

1 Introduction

1.1 In order to facilitate the development and integration of Automatic Number Plate Recognition (ANPR) systems used by law enforcement agencies (LEAs), a set of standards have been developed by the National ANPR Programme Team on behalf of the Association of Chief Police Officers of England, Wales and Northern Ireland (ACPO) and the Police Service of Scotland. These are the National ANPR Standards for Policing (NASP). The standards are consistent with the requirements of the Surveillance Camera Code of Practice issued under provisions of the Protection of Freedoms Act 2012 (PFA).
It is expected that these standards be adopted by LEAs throughout the UK.

1.2 NASP is divided into two parts:
Part 1 – Data Standards
Part 2 – ANPR Infrastructure Standards
Part 1 (published separately) prescribes the standards with which data must comply in order for it to be accepted into the police National ANPR Infrastructure (NAI).
Part 2 (this document) prescribes the standards for the components of the National ANPR Infrastructure including the operability standards required of Back Office systems that are to be used by LEAs and connected to the NAI.

1.3 NASP provides the standards that are required to be achieved by the ANPR Infrastructure in operation and therefore does not enable any component parts to be tested and accredited as 'NASP Compliant'. LEAs are responsible for ensuring that all components of infrastructure have the capability to support compliance with NASP, prior to installation. Any testing of components connected to the national ANPR Infrastructure may only be conducted with the express authority of the National ANPR Programme.

1.4 This document supersedes any previously published versions. (Last previous version was National ACPO ANPR Standards - NAAS v 4.13)

2 Applicability

2.1 These standards apply to any ANPR systems operated by the police service and other LEAs, throughout the UK, that connect to the NAI. ANPR systems include the Number Plate Reading Device (NRD), the Back Office Facility (BOF), communications links, firewalls and other related supporting components, including those components that are under the ownership or control of other organisations.

2.2 An ANPR system must conform to Parts 1 and 2 of the NASP for it to be a candidate for supplying data to the National ANPR Data Centre (NADC).

3 Data Handling

3.1 Once ANPR data is loaded onto a Police database it is deemed to be 'personal data' in the context of the Data Protection Act 1998 (DPA) and therefore, all ANPR data within police databases should be handled in accordance with DPA principles.

3.2 Whilst in the custody of, or being transmitted to or from a LEA, ANPR data should be handled as follows:

a. Where the data has just been captured by an ANPR device and before it is entered onto a Police database system it is to be protected, as a minimum, in transit either by commercial standard encryption or be sent unencrypted over a network accredited to process PROTECT data.

b. Where the data has just been entered onto a Police database system it is to be protected, as a minimum, in transit either by an agreed commercial standard encryption or be sent over a network accredited to process RESTRICTED data in accordance with the Government Protective Marking Scheme (GPMS).

4 Related Requirements

4.1 ANPR Infrastructure Development

ANPR NRD may only be deployed, or an LEA receive data from ANPR systems operated by other organisations, at locations identified following a strategic assessment that identifies a need for ANPR at that location in order to detect, deter, and disrupt criminality. Where a need is identified consideration of whether the deployment, or receipt of data, is appropriate and proportionate in balancing protection of the public with the rights and legitimate expectations of individual privacy is also required. Strategic assessment should take account of the following factors:

- National Security and Counter Terrorism,
- Serious, Organised and Major Crime
- Local Crime,
- Community Confidence and Reassurance, Crime Prevention and Reduction.

A Privacy Impact Assessment (PIA), which will include consultations with relevant stakeholders, is required for all planned new infrastructure. The extent of consultation should be determined in the context of the proposed development, with a presumption that it will include all persons and organisations with a reasonable interest in the proposal unless that would be contrary to the purpose of the development, namely, to detect, deter, and disrupt criminality, or the deployment is covert authorised within provisions of the Regulation of Investigatory Powers Act 2000 (RIPA) or the Regulation of Investigatory Powers (Scotland) Act 2000 (RIPSA).

The continued requirement for NRD at a location, or for an LEA to receive data from ANPR systems operated by other organisations, should be monitored and the device removed, or the receipt of data terminate, should the justification for deployment at that location cease. The locations of all NRD, and need to receive data from systems operated by other organisations, must be reviewed annually taking account of the above factors to ensure that the deployment, or receipt of data, remains appropriate and proportionate.

4.2 NASP Data Standards

All ANPR systems must handle data in conformance with Part 1 of the NASP.

4.3 NADC Code of Connection (NADC CoCo)

All ANPR systems must conform to the requirements of the NADC CoCo and any connection to NADC must be in accordance with issued web services standards (8.5 post). Where relevant, submission of a completed Community Code of Connection may provide sufficient assurance.

4.4 Schengen Information Systems (SIS)

All ANPR systems must meet the requirements of SIS II when the Schengen Information Systems come into operation and must be capable of reading plates that form part of the Schengen community, including Northern Ireland and Republic of Ireland plates.

5 Accreditation

In order to preserve the integrity of the NAI, all BOFs must be assessed to ensure that they do not pose a threat to the national infrastructure and are suitably for handling data up to GPMS RESTRICTED level.

5.1 LEA domain

The assessment of risk to an LEA domain rests with the Chief Officer for each LEA, which will normally be discharged by the Information Security Officer (ISO) for that LEA. The level of risk posed should be determined through completion of a HMG IS2 compliant Risk Management and Accreditation Document Set and an IT health check.

5.2 Criminal Justice Extranet (CJX)

The National Accreditor for Police Systems (NAPS) needs to be assured that the BOF service poses no threat to the CJX community. The NAPS will liaise with the LEA ISO to assess the level of risk posed, as documented through the Force corporate RMADS and Health Check process, and determine whether the BOF is approved for connection to the CJX. This is confirmed by completion of the Community Code of Connection and/or NADC CoCo.

5.3 BOF Accreditation

Once one LEA has undertaken the accreditation of a particular BOF, the NAPS will determine under what conditions a particular accreditation may be extended to apply to the use of the product by other LEAs.

6 System Types

The performance standards for NRD shown below are most easily met for vehicles travelling towards a NRD, and it is recommended that unless unavoidable, e.g for some dual lane deployments, that this configuration is used in all cases.

6.1 Static ANPR Systems

A static ANPR system is one that has been built for the primary purpose of 'capturing' and 'reading' vehicle registration marks (VRMs) and is located in a fixed position with no intention of the system being moved. Except in extreme weather conditions the performance standards for these systems must be achieved at all times. Systems must capture 98% of all VRM that are visible to the human eye[1] and accurately read 95% of captured VRM.

6.2 Moveable ANPR Systems

A moveable ANPR system is one that has been built for the primary purpose of 'capturing' and 'reading' vehicle registration marks (VRMs) and is located in a fixed position on a temporary basis. Except in extreme weather conditions the performance standards for these systems must be achieved at all times. Systems must capture 98%

[1] 'Visible to the Human eye' should be determined from the viewpoint of the camera within the ANPR system. A number plate visible to a 'human eye' at that location should also be visible by the ANPR system. Where a number plate is not displayed or it is obscured, for example by another vehicle, then it is not visible and should be discounted.

of all VRM that are visible to the human eye[2] and accurately read 95% of captured VRM.

6.3 Dual Lane ANPR Systems

A Dual Lane ANPR system is one that has the capability to read VRM for vehicles travelling in two lanes of the highway using a single NRD. Except in extreme weather conditions the performance standards for these systems must be achieved at all times. Systems must capture 98% of all VRM that are visible to the human eye and accurately read 95% of captured VRM for vehicles travelling towards the NRD. Taking account of the difficulty in configuring a dual lane NRD to maximise the capture rate for vehicles travelling in both directions of the highway, in respect of vehicles travelling away from the NRD, the system must capture 90% of all VRM that are visible to the human eye[3] and accurately read 95% of captured VRM.

6.4 CCTV Integrated ANPR Systems

A CCTV Integrated ANPR system is where a dual-purpose CCTV camera can operate as a CCTV camera and as a NRD. The camera should be optimised for the purposes of ANPR. In particular, details of the time/location/camera number must be accurately reported to the BOF. Integrated systems must only provide data to the BOF when in ANPR mode. Except in extreme weather conditions the performance standards for these systems must be achieved at all times when deployed in ANPR mode. Systems must capture 85% of all VRM that are visible to the human eye[4] and accurately read 95% of captured VRM.

6.5 Mobile ANPR Systems

A mobile ANPR system is one that has been built for the primary purpose of 'capturing' and 'reading' VRMs. These include vehicle-mounted ANPR systems and other portable systems deployed on a temporary basis. Any equipment procured after the publication of this version of NASP must be live-linked to the BOF. To achieve the optimum performance requirements, mobile equipment should be capable of night-time and low-light operation. Except in extreme weather conditions the performance standards for these systems must be achieved at all times. Systems must capture 98% of all VRM that are visible to the human eye[5] and accurately read 95% of captured VRM unless deployed in a moving vehicle when the system must capture 80% of all VRM that are visible to the Human eye[6] and accurately read 95% of those captured.

6.6 Covert Systems

It is recognised that circumstances may arise where temporary static, portable systems or purpose built covert systems are deployed in support of an investigation in circumstances where it is not possible to establish a live-link to the BOF. Deployments of this type that are authorised within provisions of the RIPA or RIPSA are the only circumstances, where equipment procured after the publication of this version of NASP, may not have the capability to live-link to the BOF. Except in extreme weather conditions the performance standards for these systems must be achieved at all times.

---

[2] See footnote 1 ante.

[3] See footnote 1 ante.

[4] See footnote 1 ante.

[5] See footnote 1 ante.

[6] See footnote 1 ante.

Systems must capture 98% of all VRM that are visible to the human eye[7] and accurately read 95% of captured VRM.

7 System Capability and Resilience

7.1 Image Capture

All ANPR systems under the ownership or control of LEAs must have the capability to capture and record supporting imagery. The ability to record a plate patch image is mandatory, and an overview image is optional. Number Plate Reading Devices (NRD) operated by other organisations that are not enabled for the recording of imagery may be connected to the ANPR infrastructure operated by an LEA. Supporting Images are important to assist with the accuracy of individual capture records and therefore, where an LEA receives data from other organisations without supporting images provision for upgrading of the system to enable the provision of images should be established.

7.2 Centralised Data Storage

ANPR data should be stored in locations to provide both a Primary System and a Backup or Disaster Recovery System.
Textual ANPR data may be stored on one hardware environment with related images stored on a separate hardware environment that is optimised for the storage of images.

7.3 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 72 hours, should the BOF or communications to the BOF become unavailable. In the event of a failure to send capture records and images to the NADC systems must have the capability to buffer and re-send that data.

7.4 Mobile ANPR Systems Data Transfer

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

7.5 Mean Time between Failure

All ANPR systems must have a mean time between failures of any components of the system of not less than 5,000 hours and a minimum availability of 99.5%.

7.6 Support and Maintenance

ANPR systems should be commissioned only with an appropriate level of support and maintenance to safeguard against component failure and assist with business change. It is recommended that Back Office suppliers are able to provide support remotely through Secure Communities Networks (SCN). Such suppliers will have to comply with, and complete a Community Code of Connection.

[7] See footnote 1 ante.

8 System Connectivity

8.1 BOF Connectivity to LEA Networks and to CJX

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

8.1.2 The security of all connections to the BOF must be managed via an organisation maintained and managed firewall in accordance with that organisation's own policy and the Community Code of Connection and ACPO/ACPOS Community Security Policy.

8.2 National Databases

8.2.1 BOF must have the capacity to run the following national databases, as a minimum:

- PNC; Includes 'Fast Track' 'Extract' and 'Schengen'
- Driver and Vehicle Licensing Agency (DVLA) (no current keeper and no VEL)
- Motor Insurance Database (MIDAS)

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

8.3 Real-Time Matching

8.3.1 The BOF must provide real-time matching to PNC (#RE Fast Track) and other hotlists for all ANPR reads.

8.3.2 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 and CCTV Integrated systems, and **6 seconds** for mobile ANPR systems.

8.3.3 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, Moveable and CCTV ANPR Integrated systems and within **4 seconds** of capture for Mobile ANPR systems.

8.3.4 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 following table summarises maximum system response times.

System Type	Read to alarm	Number plate capture to delivery to BOF	BOF process to delivery
Static ANPR system	4 sec	2 sec	2 sec
CCTV Integrated ANPR system	4 sec	2 sec	2 sec
Mobile ANPR system	6 sec	4 sec	2 sec

8.4 Real-Time Data Delivery

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

8.4.2 The BOF must clearly display the current state of connectivity to the NADC and/or any time when data is not being sent to the NADC. In the event of a communications or systems failure, the BOF must buffer that read data and deliver it to the NADC, once the communications or failed systems have been restored. The real-time delivery of data is a priority and the delivery of any buffered data should take place in addition to delivery of real-time data.

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

- local – TCP/IP over the LEA network
- regional – wireless transmission
- national – CJX from forces, PNC and the national ANPR systems.

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

8.5 Search and Export of Data

8.5.1 The BOF must provide for the identification and export of data that may be identified using any of the following criteria:

- Vehicle Registration Mark (VRM);
- Date and time parameters;
- by camera identification;
- by location co-ordinates;
- by ‘geo plotting’

8.5.2 Data is to be exported in CSV format, Images in Jpeg format.

8.5.3 Bulk data, including images, required for investigative purposes that may be stored under provisions of the Criminal Procedure and Investigation Act 1996 (CPIA) is to be exported to an external LEA defined storage area in xml format and managed in accordance with local policy.

8.5.4 The BOF must provide for user defined privileges for use of data export functions.

8.6 Web Services

8.6.1 Compliance with Web services specifications are a requirement of the NASP. They provide essential information to describe the interfaces required for connecting to other BOFs and to source equipment for the transfer of information.

8.6.2 Web services are also used 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.

8.6.3 Current versions of web services specifications for ANPR systems are defined by the National ANPR Programme and are held by the National ANPR Programme Team.

8.7 Interoperability

8.7.1 Systems must enable interoperability between other LEA BOFs and NADC to allow:

- real-time matching of reads against hotlists and the real-time delivery of hits
- remote BOF research in accordance with prevailing researching guidelines

- 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).
- hotlist distribution to other LEA BOFs and NADC
- access to and the transfer of data and all associated images between other LEA BOFs and NADC.

8.8 Security

8.8.1 The BOF must provide adequate security measures, including access control, to protect against unauthorised access to the system and data held within it. LEA must ensure that Individual user privileges are consistent with the requirements of their role and individual level of security vetting.

8.8.2 Audit trails must be maintained to record all significant actions taken, including user login, both successful and failed database searches, and the addition to, and deletion of data from hotlists. There must be provision within the BOF for users to record the reasons for their actions. Access to audit trails must also be auditable and restricted to users who require this access as part of their role, and defined within policy.

8.8.3 The security of all connections to the BOF must be managed via an LEA maintained and managed firewall in accordance with the LEA's own policy and the Community Code of Connection and Community Security Policy.

8.8.4 The BOF server must be protected from NOT PROTECTIVELY MARKED networks by a CESG approved E3/EAL4 accredited firewall, configured to protect access to the system from unauthorised external connections.

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

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

9 Databases

9.1 PNC Extract File

9.1.1 The PNC Extract File is available to forces at least three times 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.

9.2 Third Party Databases

9.2.2 Where data is provided by a third party (e.g. the PNC Extract File as provided directly/indirectly from PNC), then the LEA 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:

- Any onward distribution to any third party (individual and/or system) must be done using secure and auditable methods.
- Provisions must be in place to ensure that only the most up-to-date data set is in use.
- Version control and file naming systems must be in place
- Distribution methods must be in accordance with GPMS security requirements.
- Data must not be provided to non-LEA personnel unless specifically authorised by an officer of ACPO rank (or equivalent) within the LEA

9.3 Local Hotlists

9.3.1 The contents of hotlists will be dependant upon the purpose of the list. Those used for monitoring purposes that do not require an operational response may include minimal details, when used to support operational response sufficient information to ensure appropriate response must be included. A local ANPR Hotlist should only be used in circumstances that do not meet the standards for inclusion on the PNC.

9.3.2 LEA may agree to supply each other with their appropriate local ANPR Hotlist(s) to facilitate cross-border policing activity in support of identified policing priorities, provided that each undertakes, subject to local resource availability and operational demands, to monitor the shared hotlists, to assess a 'hit' against a supplied list on its own merit and to respond in accordance with current policy in the force that receives the report of a 'hit'.

9.3.3 The LEA supplying a hotlist must ensure that a information within a hotlist supplied to another organisation within the terms of his MOU is accurate, of current relevance, and is in a format that conforms to the requirements detailed within NASP. All hotlists that are supplied to another organisation will be reviewed on a regular basis by the LEA| supplying the list, and any revised list circulated to the other organisation within 24hours of revision.

9.3.4 A hotlist that is received from another LEA will cease to be used by receiving LEA on receipt of a revised version of that list, or for a maximum of 28days following the last date of revision by the LEA that supplies the list, whichever occurs first.

9.3.5 The LEA receiving a local hotlist for response purposes will not extract data from that list for the purposes of creating a composite list for response purposes.
All hotlists must conform to the following template, **(Mandatory elements shown in bold text)**:

Column	Description	Standard Words	Comment
1	**VRM**		No Spaces
2	MAKE		
3	MODEL		
4	COLOUR		

Column	Description	Standard Words	Comment
5	ACTION 1ST WORD	Stop Assess No Alert	Action can include a requirement to STOP the vehicle and take action as described or to Assess in the context at the time the vehicle comes to notice to determine action. (No alert to be used when a hotlist is submitted for monitoring purposes with no intention that action is taken when the vehicle comes to notice. A Directed Surveillance Authority (DSA) may be required.)
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	Crime Disqualified Drink Drive Documents Drugs Intel Sexual VISOR Other	
8	INTEL 5X5X5		Enter grading without X or spaces
9	INFORMATION/ ACTION	Prefix free text with date and time in format shown in 2.1.2 (above)	Brief free text to include and additional information and Force reference number if applicable and date information/ intelligence became available
10	**FORCE AND AREA**		Include Force Name/ Area (BCU/Division letter) and 24hr contact tel no.

Column	Description	Standard Words	Comment
11	**WEED DATE**	Provide date and time in format [dd/mm/yyyy], entries will be weeded on the day specified.	
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		

10 Data Management and Access Control

10.1 Policy

10.1.1 Written policy must be in place detailing the requirements for data management and access control including provisions for audit.

10.2 Record Retention and Deletion

10.2.1 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 CPIA, or similar provisions in Scotland, alternative retention periods are appropriate.

10.2.2 Functionality must be in place to enable the management and deletion of data within ANPR systems. In particular the BOF must provide for the deletion of:

- capture records, after a default time that is user-configurable
- hotlists, according to the weed date set for each individual hotlist
- hotlist entries, according to the weed date set for each individual hotlist entry. The weed date may be set for a maximum period of 28 days from initial entry onto a hotlist or following the date of a review that has been conducted for that entry where the accuracy and continued requirement for the entry has been confirmed.

10.2.3 The BOF must also allow for capture records to be marked as immune from weeding, so that they are retained for investigative purposes. There must be functionality that allows immunity to be removed from records.

10.3 Access Control

10.3.1 Provisions for access to ANPR data held on local databases must be detailed within an organisations policy taking account of the requirements of legislation. It is recommended that local policy is consistent with requirements for access to other ANPR databases. PNC, DVLA and ANPR data is 'Personal Information' as defined by the Data Protection Act 1998 and force policy for access to other ANPR databases must be consistent with the following.

10.3.2 Access to data held on NADC or other LEA Systems

I. The ANPR Chief Officer lead within an organisation will designate a member of staff of at least Superintendent rank (or equivalent staff grade) who is accountable for the authorisation of staff who may access ANPR systems owned by other LEA, or the NADC for investigation or intelligence purposes.

II. Authorised members of staff will be in investigation or intelligence roles and limited to a number of people proportionate to the extent that access is required. Organisations must ensure that authorised staff are fully aware of the provisions of NASP and current Memoranda of Understanding (MOU) for access to data, as relevant to their role.

III. LEA will maintain a list of authorised staff and ensure that a persons' authorisation is cancelled if they cease to be employed in a relevant investigation or intelligence role.

IV. Organisations will maintain records, and audit the access to other organisations databases to ensure compliance with provisions within NASP and MOU and maintain records of access and audit in a readily retrievable form.

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.

'Real Time'	When monitoring alarms relating to a list of vehicles (hot list) posted on NADC.	Any member of staff authorised to receive reports against the hot list with no additional authority required. (This is automated functionality within ANPR systems)
Up to 90 Days	Counter Terrorism Investigations Major Investigations Serious Investigations Specific Vehicle Registration Marks (VRM) for Priority and Volume Investigations (Recordable Offences only) [Appendix A]	Any member of staff authorised to access ANPR systems owned by other LEA, or the NADC with written request from another member of staff who is accountable for the investigation.
91 Days to 1 year	Counter Terrorism Investigations Major Investigations Serious Investigations [Appendix A]	Any member of staff authorised to access ANPR systems owned by other LEA, or the NADC with written authority of Superintendent or equivalent staff grade, who is not directly connected with the conduct of the investigation.
1 year and over	Counter Terrorism Investigations Major Investigations	Any member of staff authorised to access ANPR systems owned by other LEA, or the NADC with written authority of Superintendent or equivalent staff grade, who is not directly connected with the conduct of the investigation.

NB: Access to data held on the NADC or other LEA systems data in relation to Priority and Volume Investigations is limited to only the investigation of recordable offences and not all investigations that are included within the definition (Appendix B). Searching is also limited to investigation of a specific VRM. (which may include a partial VRM)

11 Performance Evaluation

11.1 Unless para 11.4 applies, on installation of any component of ANPR Infrastructure compliance with performance standards detailed within NASP must be confirmed and recorded. This is required on initial installation or on re-installation or re-deployment of any ANPR camera or other component. Any assessment of 'capture' rate must be based on not less than 250 consecutive vehicles (or a minimum period of 2 hours) displaying a VRM visible to the human eye passing within the field of view for a NRD. The 'read' rate must be determined for not less than 250 consecutive 'captured' Vehicles displaying a VRM visible to the human eye. Performance must be assessed for daylight and night time conditions. It is advisable to assess for a range of conditions including; bright daylight (dawn); bright daylight (dusk); overcast daylight and night time.

11.2 An annual performance evaluation of all ANPR systems must be conducted to assure conformance with the data standards defined in this document. Timescales for audit must be defined in local policy and standard operating procedures.

11.3 Performance must be consistent with guidance, provided by the Home Office Centre for Applied Science and Technology (CAST) that is current at the time of assessment.

11.4 Where covert installation of ANPR infrastructure has been authorised within the provisions of RIPA, and the purpose of the installation may be compromised as a result of testing, the testing need not be completed.

12 Further Details

Any enquires in relation to NASP should be addressed in the first instance to the National ANPR Programme Team at anpr@homeoffice.gsi.gov.uk.

Glossary of Terms, Abbreviations and Definitions

ABH	Actual Bodily Harm
ANPR	Automatic Number Plate Recognition
ANPR system	A collection of cameras, readers and Back Office Facility
BOF	Back Office Facility
Capture	The process by which a VRM is read
CAST	Home Office Centre for Applied Science and Technology
CCTV	Closed Circuit Television
CorDM	Police Corporate Data Model
CESG	National Technical Authority for Information Assurance
CPIA	Criminal Procedure and Investigations Act 1996
CJX	Criminal Justice Extranet
CTC	Counter Terrorism Check
DPA	Data Protection Act 1998
DVLA	Driver and Vehicle Licensing Agency
Fast Track	Real time matching against PNC (#RE transaction)
ISO	Information Security Officer
FIS	Force Intelligence System
Geo Plotting	The selection of an area on a map to identify location criteria for the export of data
GIS	Geographical Information System
GPMS	Government Protective Marking Scheme
ICO	Information Commissioner's Office
ISS4PS	Information Systems Strategy for the Police Service
LEA	Law Enforcement Agency
MIDAS	Motor Insurance Database
MOU	Memorandum of Understanding
NASP	National ANPR Standards for Policing
NADC	National ANPR Data Centre
NAI	National ANPR Infrastructure
NRD	Number Plate Reading Device

PFA	Protection of Freedoms Act 2012
Plate Patch	An image showing the number plate only
PNC	Police National Computer
RIPA	Regulation of Investigatory Powers Act 2000
RIPSA	Regulation of Investigatory Powers (Scotland) Act 2000
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
SCN	Secure Communities Networks
SIO	Senior Investigating Officer
SIS	Schengen Information System
VEL	Vehicle Excise Licence
VRM	Vehicle Registration Mark
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 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 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)
Vulnerable Missing Person
Wounding (S18/20)

Serious Investigations may, with the authority of a Superintendent (or equivalent staff grade), 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 (or equivalent staff grade) be escalated to the category of Serious 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)
	• Complexity of the Investigation

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