



THE CHIEF CONSTABLE OF NORTH YORKSHIRE

Automatic Number Plate Recognition (ANPR)

FINAL

Internal audit report: 10.17/18

9 February 2018

This report is solely for the use of the persons to whom it is addressed.
To the fullest extent permitted by law, RSM Risk Assurance Services LLP
will accept no responsibility or liability in respect of this report to any other party.



CONTENTS

1 Executive summary	2
2 Detailed findings	5
Appendix A: Scope	14
Appendix B: Further information.....	16
For further information contact	17

Debrief held	6 February 2018	Internal audit team	Daniel Harris, Head of Internal Audit Angela Ward, Senior Manager Philip Church, Client Manager Dulcie Hakin, Lead Auditor
Draft report issued	9 February 2018		
Responses received	9 February 2018		
Final report issued	9 February 2018	Client sponsor	Assistant Chief Constable Chief Inspector ANPR Data, Access and Technical Manager Project Manager
		Distribution	Assistant Chief Constable Chief Inspector ANPR Data, Access and Technical Manager Project Manager

As a practising member firm of the Institute of Chartered Accountants in England and Wales (ICAEW), we are subject to its ethical and other professional requirements which are detailed at <http://www.icaew.com/en/members/regulations-standards-and-guidance>.

The matters raised in this report are only those which came to our attention during the course of our review and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made. Management actions raised for improvements should be assessed by you for their full impact before they are implemented. This report, or our work, should not be taken as a substitute for management's responsibilities for the application of sound commercial practices. We emphasise that the responsibility for a sound system of internal controls rests with management and our work should not be relied upon to identify all strengths and weaknesses that may exist. Neither should our work be relied upon to identify all circumstances of fraud and irregularity should there be any.

This report is solely for the use of the persons to whom it is addressed and for the purposes set out herein. This report should not therefore be regarded as suitable to be used or relied on by any other party wishing to acquire any rights from RSM Risk Assurance Services LLP for any purpose or in any context. Any third party which obtains access to this report or a copy and chooses to rely on it (or any part of it) will do so at its own risk. To the fullest extent permitted by law, RSM Risk Assurance Services LLP will accept no responsibility or liability in respect of this report to any other party and shall not be liable for any loss, damage or expense of whatsoever nature which is caused by any person's reliance on representations in this report.

This report is released to you on the basis that it shall not be copied, referred to or disclosed, in whole or in part (save as otherwise permitted by agreed written terms), without our prior written consent. We have no responsibility to update this report for events and circumstances occurring after the date of this report.

RSM Risk Assurance Services LLP is a limited liability partnership registered in England and Wales no. OC389499 at 6th floor, 25 Farringdon Street, London EC4A 4AB.

1 EXECUTIVE SUMMARY

1.1 Background

As part of the 2017/18 approved internal audit plan we have undertaken an audit of Automatic Number Plate Recognition on behalf of the Chief Constable of North Yorkshire to confirm if the Force is complying with National ANPR Standards for Policing (NASP), the national guidance for ANPR that all forces must comply with.

The NASP comes in three parts and covers data standards, infrastructure standards and data and access management standards. We have carried out our review with reference to these three documents.

The Force's ANPR systems are currently installed by an external company, QRO, and data collected from these devices are initially managed by the Force's ANPR Hub. On installation, the performance of ANPR devices should be measured to ensure that capture rates and read rates from the devices meet the requirements detailed in NASP. After installation, performance should be reviewed at least annually.

The decision of where to install ANPR systems is made at ANPR Deployable Camera meetings where bids for ANPR systems are submitted for approval, these take place every two months and are chaired by the Authorising Officer, this is currently a Detective Superintendent.

The National Police Chiefs' Council (NPCC) guidelines currently state that ANPR capture records must be deleted no later than two years after their initial capture date. The General Data Protection Regulation (GDPR) that is being introduced in May 2018 will require changes to this retention period and therefore current ANPR guidance. The National ANPR Centre will carry out audits of data held at each Law Enforcement Agency (LEA) to ensure they are complying with updated GDPR legislation, we did not cover the impact of GDPR or the Force's plans for GDPR changes in this audit.

1.2 Conclusion

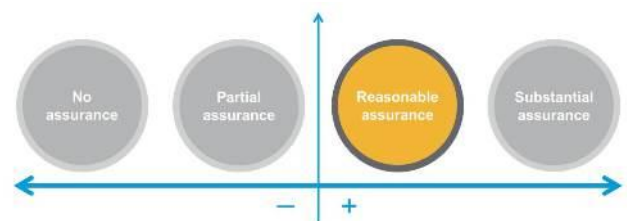
The strategic threats and operational need for ANPR deployment had been fully considered for our sample and the capture records were compliant with NPCC guidelines. However, our review found that Individual Privacy Impact Assessments were not being completed, provisions for audits on access control were not detailed in the Force's policy documents, and due to delays in moving processes in-house, initial and annual assessments of performance of ANPR devices had not been carried out.

We have agreed **three medium** and two low priority management actions in relation to these findings. Further details of our findings and actions can be found in section two of this report.

Internal audit opinion:

Taking account of the issues identified, the Chief Constable of North Yorkshire can take **reasonable assurance** that the controls to manage this area are suitably designed and consistently applied.

However, we have identified issues that that need to be addressed in order to ensure that the control framework is effective in managing this area.



1.3 Key findings

The key findings from this review are as follows:

- The ANPR Policy and ANPR Procedure documents were reviewed in line with NASP, we found they sufficiently covered contents of NASP.
- For the deployed ANPR devices we tested that were approved at ANPR Re-Deployable Camera meetings there was an ANPR Re-Deployable Camera Request for Deployment document that detailed the need for ANPR at the location, types of crimes that would be targeted and community reassurance from the installation of the device.
- ANPR capture records held on the Cleartone system which are automatically deleted after two years, so the Force is compliant with NPCC guidelines that state capture records must be deleted no later than two years after their capture.
- When staff perform a search on capture records that have been held on the system for more than 90 days since their capture, the system automatically prompts them to enter an authoriser and reason for the search.

We have agreed five management actions in relation to the following seven findings:

- Some of the ANPR deployments in our sample had been approved outside of ANPR Deployable Camera meetings and they were not always documented in the minutes following.
- The reviews of deployed ANPR devices were not always carried out in the review timeframe assigned on approval.
- There was an overarching Privacy Impact Assessment (PIA) in place for the Force, however it had not been reviewed since September 2015.
- There was not an individual PIA for each ANPR system currently deployed, despite NASP stating that a PIA is required for all planned ANPR infrastructure.
- The standalone ANPR Data Storage, Access and Management document had an out of date list of functions with access to ANPR data and was unclear of how access control audits would be carried out and what evidence needed to be retained for these audits. Discussions during our review also found that these audits were not actually being carried out.
- For internal requests for searches on capture data that have been on the system for more than 90 days, evidence of approval of these searches were not retained for the sample we tested. It also became apparent during our audit that staff were not aware of who could authorise searches on capture records.
- When ANPR devices were re-deployed, performance standards were not being tested. There were also no regular performance checks for devices that had been deployed for 12 months or more.

1.4 Additional information to support our conclusion

The following table highlights the number and categories of management actions made. The detailed findings section lists the specific actions agreed with management to implement.

Area	Control design not effective*		Non Compliance with controls*		Agreed actions		
					Low	Medium	High
ANPR	1	(9)	6	(9)	2	3	0
Total					2	3	0

* Shows the number of controls not adequately designed or not complied with. The number in brackets represents the total number of controls reviewed in this area.

* Our review identified seven findings, these have been addressed in five management actions.

2 DETAILED FINDINGS

Categorisation of internal audit findings

Priority	Definition
Low	There is scope for enhancing control or improving efficiency and quality.
Medium	Timely management attention is necessary. This is an internal control risk management issue that could lead to: Financial losses which could affect the effective function of a department, loss of controls or process being audited or possible regulatory scrutiny/reputational damage, negative publicity in local or regional media.
High	Immediate management attention is necessary. This is a serious internal control or risk management issue that may lead to: Substantial losses, violation of corporate strategies, policies or values, regulatory scrutiny, reputational damage, negative publicity in national or international media or adverse regulatory impact, such as loss of operating licences or material fines.

This report has been prepared by exception. Therefore, we have included in this section, only those areas of weakness in control or examples of lapses in control identified from our testing and not the outcome of all internal audit testing undertaken.

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no)	Audit findings and implications	Priority	Action for management
-----	---------	----------------------------------	---------------------------------	---------------------------------	----------	-----------------------

Area: ANPR

1	<p>Bids for deployment / re-deployment of an ANPR at a specific location are presented at ANPR Re-Deployable Camera meetings with a strategic assessment of the location.</p> <p>NASP states that strategic assessment should take account of the following factors:</p>	Yes	No	<p>We obtained a sample of 10 ANPRs currently in deployment and carried out testing to confirm if a strategic assessment had been carried out as part of the camera bid.</p> <p>Our testing found the following:</p> <ul style="list-style-type: none"> There was an ANPR Re-Deployable Camera Request for Deployment document in place for nine of the bids. In these cases the need for ANPR at that specific location had been detailed, including types of crime that would be targeted, community reassurance had also been considered. <p>Eight of the documents had all been approved at the ANPR Re-Deployable Camera meeting.</p> <p>One had been approved outside of the meeting by the Authorising Officer, however it had not been mentioned in the ANPR Re-</p>	Low	<p>A single spreadsheet will be implemented to provide an audit trail for all the Force's ANPR devices.</p> <p>This spreadsheet will include details such as the location of the device, re-deployment date, review date, date the bid was submitted and approved, if the bid was submitted outside of ANPR Camera meetings and links to any relevant documentation.</p>
---	--	-----	----	---	-----	--

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no)	Audit findings and implications	Priority	Action for management																														
	<ul style="list-style-type: none"> National Security and Counter Terrorism; Serious, Organised and Major Crime; Local Crime; and Community Confidence and Reassurance, Crime Prevention and Reduction. 			<p>Deployable Camera meeting that this had taken place after the approval. This was part of Operation Kingfisher.</p> <ul style="list-style-type: none"> For the other ANPR, a sensitive bid relating to organised crime had been submitted and approved by the Authorising Officer outside of the meetings, but was mentioned in the meeting. We were unable to review this ANPR Re-Deployable Camera Request for Deployment document due to its sensitivity. <p>If there is no audit trail of approval of ANPR bids, there is a risk the correct documentation may not have been completed, or the bid may not be appropriately approved.</p> <p>There is also a risk that members of the ANPR Re-Deployable Camera meeting are not aware the cameras are in deployment and these devices may therefore not be picked up for regular review.</p> <table border="1"> <thead> <tr> <th colspan="3">Risk Exposure</th> <th colspan="3">Root causes</th> </tr> </thead> <tbody> <tr> <td colspan="3">Risk of bid documentation not being completed or authorised correctly and ANPR devices being used that are not achieving their expected performance.</td> <td colspan="3">Lack of audit trail of approval and installation of ANPR locations.</td> </tr> <tr> <td colspan="3"></td> <td colspan="3">ANPR devices not being reviewed at assigned intervals</td> </tr> <tr> <th>Probability</th> <th>Financial</th> <th>Reputational</th> <th>Operational</th> <th>Legal</th> <th>Rating</th> </tr> <tr> <td>Probable</td> <td>Negligible</td> <td>Minor</td> <td>Minor</td> <td>Minor</td> <td>5:4</td> </tr> </tbody> </table>	Risk Exposure			Root causes			Risk of bid documentation not being completed or authorised correctly and ANPR devices being used that are not achieving their expected performance.			Lack of audit trail of approval and installation of ANPR locations.						ANPR devices not being reviewed at assigned intervals			Probability	Financial	Reputational	Operational	Legal	Rating	Probable	Negligible	Minor	Minor	Minor	5:4		<p>Responsible Officer:</p> <p>ANPR Data, Access and Technical Manager</p> <p>Implementation Date:</p> <p>April 2018</p>
Risk Exposure			Root causes																																	
Risk of bid documentation not being completed or authorised correctly and ANPR devices being used that are not achieving their expected performance.			Lack of audit trail of approval and installation of ANPR locations.																																	
			ANPR devices not being reviewed at assigned intervals																																	
Probability	Financial	Reputational	Operational	Legal	Rating																															
Probable	Negligible	Minor	Minor	Minor	5:4																															
2	There is an overarching North Yorkshire Police ANPR Infrastructure Development Privacy	Yes	No	<p>We confirmed there was an overarching North Yorkshire Police ANPR Infrastructure Development Privacy Impact Assessment.</p> <p>The document included the following:</p>	Low	The overarching IPA document will be reviewed to ensure it is up-to-date and it will be signed off appropriately																														

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no)	Audit findings and implications	Priority	Action for management
-----	---------	----------------------------------	---------------------------------	---------------------------------	----------	-----------------------

Impact Assessment in place.

Section A - Description of proposed ANPR Development.

This included an outline of why ANPR is used and what success criteria would be used,

Section B - Privacy Impact Assessment

This had been completed by the Force's Police Lawyer (Civil Disclosure) in September 2015. The assessment had two parts: part one was screening questions and part two was an overview of the proposed development of ANPR use in North Yorkshire, including reasons for development, and who had been consulted, both internally and externally, in the completion of the Assessment

Section C - Privacy Risks

This section detailed a table of privacy risks and solutions and results of these risks.

There was no evidence that this document had been reviewed since it was first completed in September 2015.

If the Privacy Impact document is not reviewed regularly there is a risk it may be out of date, privacy risks may not be identified and included in the risk table

Risk Exposure			Root causes		
Privacy risks may not be identified, therefore solutions will not be put in place.			Privacy Impact document is out-of-date and had not been signed off.		
Probability	Financial	Reputational	Operational	Legal	Rating
Probable	Negligible	Significant	Minor	Minor	3:13

Responsible Officer:

Chief Inspector

Implementation Date:

April 2018

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no)	Audit findings and implications	Priority	Action for management
3	<p>Missing Control</p> <p>Individual Privacy impact assessments had not been carried out for individual ANPRs at separate locations.</p> <p>NASP states that 'A Privacy Impact Assessment (PIA), which will include consultations with relevant stakeholders, is required for all planned new infrastructure.'</p>	No	-	<p>The overarching North Yorkshire Police ANPR Infrastructure Development Privacy Impact Assessment document states that re-deployable cameras will be used 'based on evidence and consideration of privacy before each deployment'.</p> <p>We confirmed the Force had a draft 'Template for ANPR Infrastructure Development Privacy Impact Assessment' document, this was due to be used for all future individual ANPR bids that go through the ANPR Re-Deployable Camera meetings to support in compliance with data protection, human rights obligations and privacy expectations when developing new ANPR infrastructure. Sections included in the document were the same as the three sections included in the overarching document.</p> <p>We confirmed in the ANPR Re-Deployable Camera meeting minutes for 10th June 2016 that the Authorising Officer advised he was currently reviewing the ANPR Privacy Impact Assessment document and that a PIA was required for every ANPR deployment, however there was a change in Authorising Officer after this and it was not followed up. As part of our testing of a sample of 10 ANPR devices currently in deployment, we reviewed the strategic assessments for each bid to see if the assessments considered privacy impact. Our testing found that that privacy impact was not considered as part of the Request for Deployment documents for any of the ANPRs in our sample.</p> <p>We also reviewed the ANPR re-deployable camera meeting minutes where each bid was assessed and approved at to see if privacy was discussed at these meetings. Our testing found that although the minutes did state that review of re-deployable camera locations included a discussion of privacy impact, there was however no further detail on privacy impact of cameras detailed in the minutes.</p> <p>By not having individual privacy assessments for each ANPR deployment, NYP are not complying with National ANPR Standards. There is a risk that relevant stakeholders are not being consulted with and the impact on and expectations of individual privacy is not being considered when planning ANPR infrastructure.</p>	Medium	<p>An individual IPA document will be used for all future ANPR bids.</p> <p>Responsible Officer:</p> <p>Chief Inspector</p> <p>Implementation Date:</p> <p>Immediately</p> <p>We will carry out an exercise to complete a privacy impact assessment retrospectively for all ANPR devices currently deployed.</p> <p>Responsible Officer:</p> <p>Chief Inspector</p> <p>Implementation Date:</p> <p>April 2018</p>

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no)	Audit findings and implications						Priority	Action for management
				Risk Exposure Risk the Force is not complying with National ANPR Standards. Relevant stakeholders are not being consulted with and expectations of individual privacy is not being considered for ANPR infrastructure.			Root causes Individual privacy impact assessments are not being carried out for each ANPR deployment.				
				Probability	Financial	Reputational	Operational	Legal	Rating		
				Probable	Negligible	Significant	Minor	Significant	3:13		
4	<p>There is a stand-alone document available on an NYP sub-site for ANPR Data Storage, Access and Management.</p> <p>This document details how ANPR data is stored, accessed and authorisation of access to data, and details of who manages ANPR data.</p>	Yes	No	<p>We obtained a copy of the standalone ANPR Data Storage, Access and Management document.</p> <p>We confirmed the document did state that access was determined by role.</p> <p>The ANPR Data, Access and Technical Manager informed us during opening meeting that the functions with authorisation to ANPR data on this document was currently out of date. It is therefore unclear who should have access to ANPR data within the Force.</p> <p>Use of ANPR - The ANPR Procedure document detailed the use of ANPR data, with links to further information about the use of ANPR as an intelligence and evidence tool and as a technical tool.</p> <p>Provisions for Access - The ANPR Policy had the NASP Data Access Requirements table in appendix A, which had been taken from NASP Part 3, however it did not make it clear how audits of access control would be carried out, or what information / evidence would need to be retained to assist with these audits.</p>						Medium	<p>Staff will be reminded of the process to retain evidence of approval for all ANPR searches on data over 90 days, including those who have authority to approve searches.</p> <p>The Force's ANPR documents will be updated to detail provisions for access control audits. Audits of access to ANPR data will be carried out by the ANPR Data, Access and Technical Manager.</p> <p>We will undertake a brief exercise to ensure that no one currently has access to the Cleartone system that shouldn't.</p>
				Risk Exposure			Root causes				

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no)	Audit findings and implications	Priority	Action for management												
				<p>Unauthorised persons have access to ANPR data.</p> <p>Searches on ANPR capture records have not been authorised.</p>		<p>Responsible Officer:</p> <p>ANPR Data Access and Technical Manager</p> <p>Chief Inspector</p> <p>Implementation Date:</p> <p>February 2018</p> <p>We will then carry out a fully comprehensive exercise to review which roles should have access to the national system once ANPR data is moved over (beginning of May)</p> <p>Responsible Officer:</p> <p>ANPR Data Access and Technical Manager</p> <p>Chief Inspector</p> <p>Implementation Date:</p> <p>May 2018</p>												
				<table border="1"> <thead> <tr> <th>Probability</th> <th>Financial</th> <th>Reputational</th> <th>Operational</th> <th>Legal</th> <th>Rating</th> </tr> </thead> <tbody> <tr> <td>Probable</td> <td>Nil</td> <td>Minor</td> <td>Negligible</td> <td>Minor</td> <td>5:8</td> </tr> </tbody> </table>	Probability	Financial	Reputational	Operational	Legal	Rating	Probable	Nil	Minor	Negligible	Minor	5:8		
Probability	Financial	Reputational	Operational	Legal	Rating													
Probable	Nil	Minor	Negligible	Minor	5:8													

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no)	Audit findings and implications	Priority	Action for management
5	<p>Staff / officers have access to ANPR data according to their job role.</p> <p>There are two levels of access depending on role, one allows access to data up to 90 days, one allows access to data over 90 days, however to access this data the officer / staff must enter the officer that has authorised their access to this data, and the reason for accessing this data.</p> <p>The system is set up so that if a search is carried out over the 90-day limit by anyone, it automatically asks for details of the authoriser and the reason for the search, no matter what the access levels are for the individual carrying out the search.</p>	Yes	No	<p>We carried out testing on a sample of ten instances where ANPR data search had been completed for data over 90 days old.</p> <p>In all instances the individual that carried out the search had detailed the authoriser and the reason for the search. Nine of the searches were part of a crime investigation. One of the searches was carried out following an intelligence development.</p> <p>We requested evidence of this approval to confirm that it was provided. Our review found the following:</p> <ul style="list-style-type: none"> • There was an ANPR Data Request form or an Application for the use of ANPR Data in Evidence form completed for seven of the searches - these were all requests from other forces or national requests for data. • For one of the searches, the person that authorised the search confirmed the reason for the search, however there was no evidence provided of the original approval. • For one of the searches, the member of staff that carried out the search was on long term sick so could not provide evidence of the search, and the person that authorised the search did not respond to our request for evidence during the audit. <p>If evidence is not retained of appropriate approval for searches on ANPR data over 90 days there is a risk that appropriate approval was not actually provided and the staff / officer has searched data without the correct authorisation.</p> <p>When evidence was requested of authorisation, one of the staff that had carried out a search informed the ANPR Data, Access and Technical Manager that they were unaware that authorisation was required from anyone other than the officer requesting the search. If staff are unaware of who can authorise ANPR data searches, there is a risk that staff are approving searches who do not have the authority to do so.</p>	-	Refer to management action 4

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no)	Audit findings and implications	Priority	Action for management
-----	---------	----------------------------------	---------------------------------	---------------------------------	----------	-----------------------

6	Deployed / re-deployed ANPR devices are installed by a contractor, QRO.	Yes	No	We carried out testing on a sample of ANPR devices currently deployed to see whether a performance assessment had been completed for the device when it was first deployed / redeployed, and for devices that had been on site for over 12 months we tested to see if the performance had been tested annually.	Medium	(Note - The Force is currently awaiting the approval of the recruitment of a Support Engineer.)
---	---	-----	----	---	--------	---

When they are installed, QRO carry out compliance checks of capture rates and read rates in line with NASP performance standards.

NASP Part 2 states the following: 'Compliance with the 'read' rate for a NRD should be reviewed at least annually with a sample of not less than 250 consecutive reads, for every lane covered by the NRD. Provisions for performance evaluation must be defined in LEA policy and procedures.'

Our testing found that a performance check had been carried out on four of the devices when they had first been deployed, however the read data provided by QRO just showed the first two and last two vehicle registration marks, and it was down to NYP's ANPR back office facility (bof) to check the percentage of data captures against NASP. This method used by QRO appears to be the 'counted plates' procedure, however this is a procedure for ongoing performance measurement techniques. The 'ground truth video' procedure should be used in the first instance when an ANPR is first deployed.

The ANPR Policy stated that performance of NRD would be assessed on installation and thereafter at least annually for all NRD that provide supporting imagery and every six months for any that do not provide images in accordance with NASP Part 2, however our testing and discussions with staff found that performance was not being reviewed in accordance with policy. This was due to a delay in the Force recruiting a support Engineer and getting a NAS Test application set up and working.

The Force is currently not complying with National ANPR Standards.

Once the Support Engineer role has been filled and training provided, all ANPR Performance testing will be completed in-house in accordance with NASP and the Force's ANPR Policy.

Responsible Officer:

ANPR Data, Access and Technical Manager

Implementation Date:

September 2018

Risk Exposure			Root causes		
The Force is not complying with National ANPR Standards.			Performance checks on ANPR devices are not being carried out.		
Probability	Financial	Reputational	Operational	Legal	Rating
	Negligible	Minor	Minor	Minor	

Ref	Control	Adequate control design (yes/no)	Controls complied with (yes/no)	Audit findings and implications	Priority	Action for management
7	<p>There is an ANPR Re-Deployable Camera meeting every two months which the Force's Authorising Officer (AO) chairs.</p> <p>At this meeting, bids for deployment of ANPR devices are assessed and approved / not approved.</p> <p>Each ANPR device has a review date, where the device is reviewed to see if it has met its requirements of its original deployment or not, and if it's use should be continued or not.</p>	Yes	No	<p>For our sample of currently deployed ANPR devices, we reviewed ANPR re-deployable camera meeting minutes to test if they were reviewed regularly, in accordance with review dates.</p> <p>There is a spreadsheet submitted for review at each meeting which detailed cameras, by location, showing installation date and review date, a written summary update on its performance and the number of reads and alarms in a two-month period.</p> <p>Our testing found of the sample of 10 ANPR devices found the following</p> <ul style="list-style-type: none"> • Six had been reviewed on their appropriate review dates. • One deployment was not due for review yet at the time of our audit. • One ANPR was deployed as part of a police Operation, it was deployed in January 2017 and was not reviewed until August 2017 (seven months) there was no record of how often this should have been reviewed. • One ANPR was deployed in January 2017 and was due to be reviewed after six months, however it was not reviewed until October 2017 (nine months). • One was deployed in March 2017 and was due to be reviewed after four months, however it was not reviewed until October 2017 (seven months). <p>If ANPRs are not reviewed on the correct date, there is a risk that they may not be performing as expected and will not be removed in a timely manner, resulting in a potential ineffective use of resources as these cameras cannot be used for another bid until they are removed.</p>	-	Refer to management action 1

APPENDIX A: SCOPE

The scope below is a copy of the original document issued.

Scope of the review

The scope was planned to provide assurance on the controls and mitigations in place relating to the following area:

Objectives of the area under review

The National ANPR Standards for Policing (NASP) guidance detail the standards that are required to be met for the development and use of ANPR systems. Our review will confirm the re-deployment of ANPR systems is consistent with NASP guidance and key accountability and responsibilities have been established.

When planning the audit, the following areas for consideration and limitations were agreed:

Areas for consideration:

Our review considered the following areas in relation to the infrastructure for the re-deployment of ANPR systems:

- There was a policy / procedure in place that provided a framework for the management, deployment and use of ANPR and it reflected the national standards.
- A strategic assessment had been undertaken to identify strategic threats necessitating ANPR deployment at a specific location to detect, deter and disrupt criminality.
- Privacy impact assessments were conducted for all assets to ensure the rights of individual privacy were considered and balanced against the need to protect the public from harm.
- There was a policy in place detailing the requirements for data management and access control including provisions for audit.
- Records were retained for the appropriate periods as set out by NPCC guidelines and Information Commissioner's office. The deletion of records was appropriately approved.
- Access to data was appropriately restricted and reasons for access were recorded.
- Compliance with performance standards detailed with the NASP guidance were undertaken for the re-deployment of any ANPR device.
- The re-deployment of ANPR devices was appropriate, considered and approved.
- Appropriate governance arrangements were in place to consider the performance and re-deployment of ANPR devices.

Limitations to the scope of the audit assignment:

- Our review only focused on the re-deployment of ANPR devices. We did not consider any other ANPR projects.
- We did not consider the impact of GDPR on ANPR data or if the Force had appropriate plans in place to address this.
- We did not review the procurement of ANPR devices or if value for money had been achieved.
- Testing was completed on a sample basis so we did not confirm all ANPR infrastructures had been undertaken in accordance with National ANPR Standards for Policing (NASP).
- We did not verify the calibration of equipment for accuracy.
- Our work does not provide absolute assurance that material errors, loss or fraud do not exist.

APPENDIX B: FURTHER INFORMATION

Persons interviewed during the audit:

- ANPR Data, Access and Technical Manager
- Chief Inspector
- Project Manager

Documentation reviewed during the audit:

- ANPR Policy
- ANPR Procedure
- ANPR Infrastructure Development Privacy Impact Assessment
- ANPR Re-Deployable Camera Request for Deployment documents
- ANPR re-deployable camera meeting minutes
- ANPR Data Storage, Access and Management document
- ANPR Data Request forms
- Application for the use of ANPR Data in Evidence forms
- Guidance on ANPR Performance Assessment and Optimisation (Home Office)
- National ANPR Standards for Policing (Home Office)

FOR FURTHER INFORMATION CONTACT

Dan Harris, Head of Internal Audit

Tel: 07792 948767

Daniel.Harris@rsmuk.com

Angela Ward, Senior Manager

Tel: 07966 091471

Angela.Ward@rsmuk.com

Philip Church, Client Manager

Tel: 07528 970082

Philip.Church@rsmuk.com