

Automatic Number Plate Recognition

Executive summary

The purpose of the Automatic Number Plate Recognition (ANPR) chapter is to ensure staff maximise enforcement opportunities, as a result of preloaded alerts, and use the tool in accordance with policy and legislation.

Key, critical points for staff to note:

- Only approved ANPR deployment methods and equipment are to be used.
- ANPR equipment must only be operated by Police who have completed formal training.
- Data obtained from ANPR deployments must only be retained for 48 hours.
- The ANPR system is only as effective as the data quality relating to the alerts – staff should correct and update any discrepancies.

Overview

Introduction

Automatic Number Plate Recognition (ANPR) is a technology used to automatically identify vehicles of interest (VOI), as flagged in the National Intelligence Application (NIA), Motor Vehicle Register (MVR), and Driver Licence Register (DLR), from their number plates.

The ANPR system uses optical character recognition (OCR) to scan vehicle number plates and check them against VOI alerts. In simple terms it assists officers by negating the need to refer to lists of VOIs by informing them when such a vehicle is detected by the system. When a VOI is recognised, the system alerts the operator who can take appropriate action.

The ANPR system allows officers to enhance enforcement opportunities by focusing on high risk drivers and offenders, ie, drink drivers, unlicensed drivers and persons with warrants who are linked to a VOI.

This document sets out:

- an overview of ANPR equipment;
- approved methods of deployment; and
- the procedures to be followed during the deployment of ANPR.

Note: This chapter applies to Police constables and authorised officers, hereafter referred to collectively as 'Police'.

ANPR equipment

Components

ANPR systems are made up of these components:

- a camera;
- a computer; and
- a monitor.

Software

ANPR systems use software which has limited support from the Police Information and Communication Technology (CT) helpdesk. Instructions on software operation and support contacts are included in the training given to ANPR operators.

Servicing

Instructions on software and hardware servicing are included in the ANPR operator manual.

ANPR vehicles

ANPR equipment must only be operated in purpose built ANPR vehicles in accordance with this Police Manual chapter. If it is operationally necessary to alter the vehicle or operate ANPR in any other manner, pre approval must be gained from the National Manager: Road Policing prior to any change being made or organised – refer to the '[Police vehicle management](#)' chapter.

Training

ANPR equipment must only be operated by Police who have completed formal training from Road Policing Support staff, or have received formal training from an employee in their district who has used ANPR, and is competent in its use. To ensure national consistency and quality of content and delivery, all training must:

- be approved by the National Manager: Road Policing; and
- comply with the quality assurance standards set by the Police Training Service Centre (TSC).

Roles and responsibilities

This table sets out the roles and responsibilities associated with ANPR equipment.

Role	Responsibilities
National Manager: Road Policing	<ul style="list-style-type: none"> • Must approve the ANPR training session content. • May approve (in writing) requests to operate ANPR in non standard deployments or outside of these guidelines.
District Commanders	Must ensure Police are trained to operate ANPR equipment prior to authorising operational deployment.
Officer in charge of ANPR operations	Must ensure all operational deployments of ANPR: <ul style="list-style-type: none"> • have a trained ANPR operator; • are used in a manner that enhances road safety and enforcement opportunities; and • maintain business as usual.
ANPR operator	<ul style="list-style-type: none"> • Must have completed an ANPR training session. • Must have read and understood the ANPR operator manual.
ANPR vehicle	<ul style="list-style-type: none"> • Must not be altered except by prior written approval from the National Manager: Road Policing. • Vans must be used as a category D vehicle and not be used to transport or hold prisoners. • Marked patrol vehicles fitted with ANPR are still a category A vehicle.
Support vehicles	These must be category A or B patrol vehicles. They should be operated by gold classified drivers .
ANPR Intercept Team	Must be aware of their powers when acting on a VOI alert as identified by ANPR.

ANPR operations - approved deployment models

Download the ANPR operations approved deployment models:




[ANPR_operations_-_approved_deployment_models.doc](#)

59 KB

Pre-deployment procedures

All deployment types

Follow these steps for all deployment types.

Step	Action
1	<p>Ensure appropriate Police resources are available to conduct the type of approved deployment:</p> <p> ANPR_operations_-_approved_deployment_modes.doc 59 KB</p>
2	Conduct a briefing on Police roles, responsibilities and operational focus, ie, high risk drivers.
3	Ensure the <u>ANPR</u> equipment is ready to operate. The ANPR van also requires the batteries to be checked.
4	Ensure the <u>ANPR</u> operator obtains an up to date begin shift folder containing the latest alerts.
5	<p>Ensure the <u>ANPR</u> camera is set up correctly:</p> <ul style="list-style-type: none"> • For static deployments, set up the ANPR vehicle ensuring it is legally and safely parked. The vehicle's position must not disrupt the normal flow of traffic. • For mobile deployments where cars may be parked, the vehicle's camera angles may be adjusted prior to arriving at the deployment location. <p>Note: Sometimes <u>ANPR</u> is best suited in the middle of the road, scanning both lanes (oncoming / away).</p>
6	Inform the Communication Centre (Comms) of the nature and location of the ANPR deployment.

Limited scale deployments

Follow these steps for limited scale deployments.

Step	Action
1	For mobile deployments, ensure the <u>ANPR</u> vehicle driver does not monitor the ANPR equipment while driving. If you are one up, pull over before checking the <u>VOI</u> alert.

Checkpoints

Follow these steps for checkpoints.

Step	Action
1	Prepare a deployment plan including a site plan .
2	Ensure adequate signage and cones are available.
3	The <u>ANPR</u> operator must ensure the intercept vehicles and checkpoint Police are in position and ready prior to commencing a deployment.

Mobile deployments

Follow these steps for mobile deployments.

Step	Action
1	For mobile deployments, ensure the <u>ANPR</u> vehicle driver does not monitor the ANPR equipment while driving.

Non-standard deployments

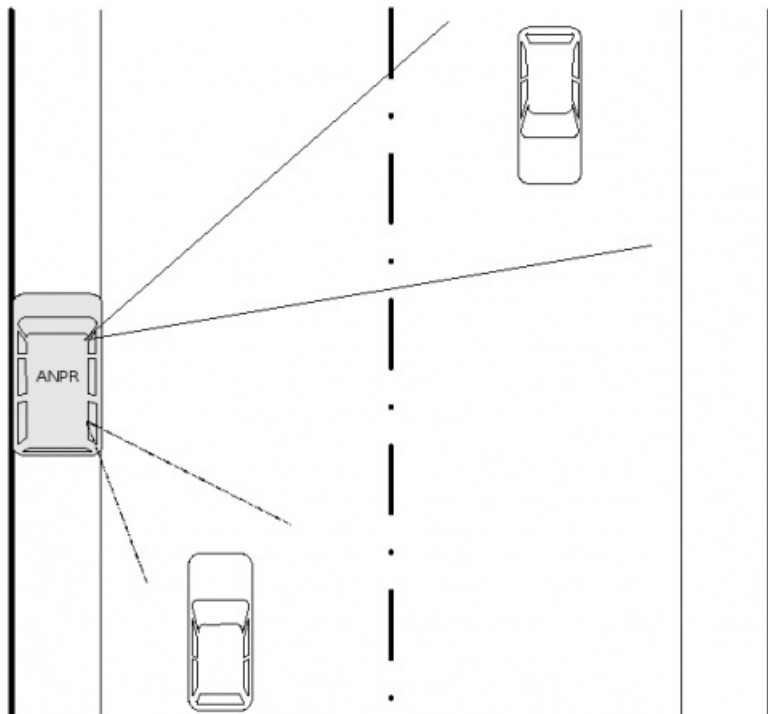
For non standard deployments, such as Impairment Prevention Teams, comply with their standard operating procedures.

ANPR deployment site plan examples

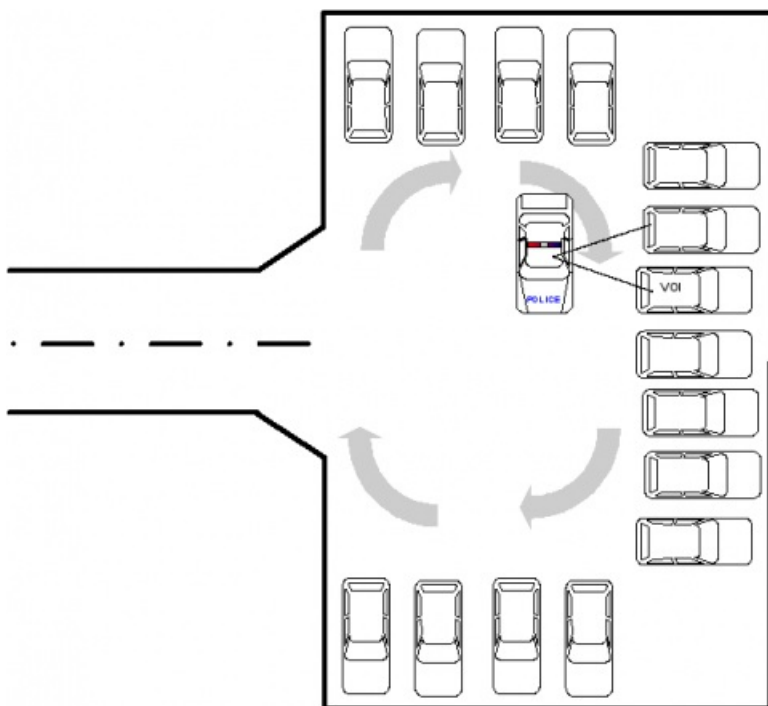
Generic examples

These are generic examples to assist the officer in charge of an ANPR operation with the preparation of site plans. For Impairment Prevention Team checkpoints refer to the '[Alcohol and drug impaired driving](#)' chapter.

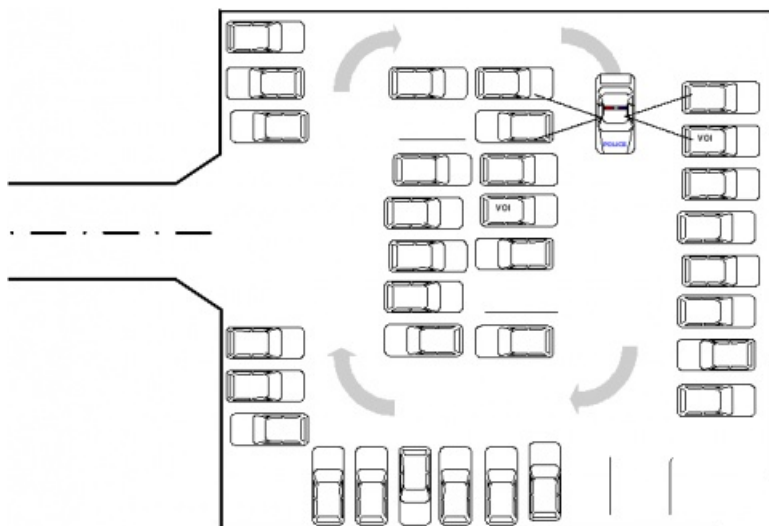
Parked deployment



Car park deployment

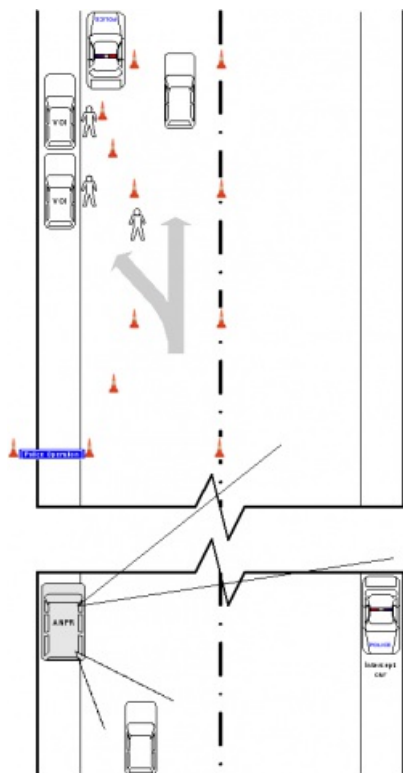


Left parking mode



Dual parking mode

ANPR checkpoint




Single/dual traffic direction mode

Note: The ANPR van/marked patrol vehicle can be set to read traffic in both directions where the checkpoint operates in both traffic directions.

Selecting a location

Points to consider

When selecting a location for all deployment types consider the Police Manual chapter [Perimeter control](#). For ANPR checkpoints also consider this table.

Consider	Rationale
The deployment model (see below)	Not all deployment models are suitable for all locations.
 ANPR_operations_-_approved_deployment_models.doc 59 KB	
Traffic volumes	To maximise the potential of ANPR, higher volumes of traffic are recommended. Only a small percentage of vehicles have VOI alerts.
Intercept risks	Consider deployment sites which allow easy migration of the ANPR or intercept vehicle into traffic flow and limit an offender's escape routes. Areas with side roads or additional potential for offenders to do u turns increase intercept risks.
Officer/public safety	Avoid areas where drivers have little reaction time prior to arriving at a checkpoint, or there is a risk of nose to tail crashes if traffic begins to queue. Avoid areas with poor overhead lights at night.
Hazard creation	The ANPR vehicle should be legally parked and in a manner that ensures the operator's and public safety.
Service disruption	<p>Avoid checkpoints that disrupt the flow of emergency service vehicles, e.g. near Police or fire stations.</p> <p>When operating with a Impairment Prevention Team ensure the ANPR intercept team operates behind the Impairment Prevention Team.</p>
Sufficient room for the intercept team and vehicles	The intercept team needs enough space to safely process VOIs, including room to tow impounded vehicles.
Local knowledge	Police will know areas where successful operations have been conducted in the past.

ANPR checkpoint procedure

Radio procedures

Where possible, only use Mobility devices for communications to limit radio traffic. Follow these steps (not necessarily in the order shown here).

Step	Action
1	Ensure Comms are aware of the nature and location of the ANPR deployment and at least one member of the intercept team monitors the main radio channel.
2	Ensure support vehicle radios remain on the main radio channel so that communication is on the main channel if an offender fails to stop when signalled to do so. For further information refer to the ' Radio and Communication Centre Protocols ' chapter.
3	Use a closed simplex channel for communication between the ANPR operator and intercept team. This channel should be kept free to allow the ANPR operators to broadcast the VOI alert type and description.

Note: The intercept team should only communicate to acknowledge the VOI alert or when they are all busy and do not require further alerts to be broadcast.

ANPR equipment setup

Refer to the ANPR Operator Manual.

ANPR checkpoint setup

Follow the [site plan](#) and for positions of the ANPR vehicle, support vehicles, signage and cones.

VOI alerts - ANPR operators

ANPR operators must follow the procedure in figure 1 below when a VOI is detected.

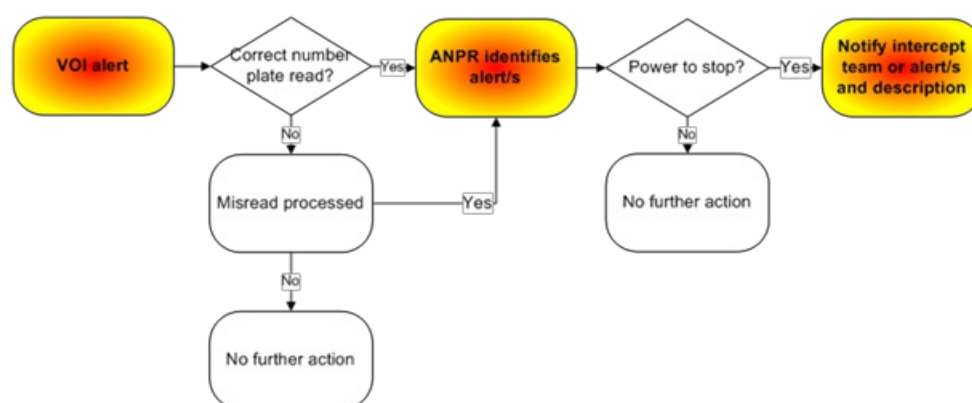


Figure 1: ANPR operators' decision chart

Plate misreads

The ANPR OCR software may occasionally misread similar shaped characters such as a '1' as an 'l', or an 'O' as a 'Q'. The ANPR operator must compare the photograph of the captured plate with the OCR definition to determine if the plate has been read correctly.

Multiple VOI alerts

The ANPR software does not prioritise VOI alerts in order of seriousness, where a detected vehicle has multiple VOI entries. Prior to informing an intercept team of VOI activity, all VOI alerts for the detected vehicle must be assessed and prioritised. The ANPR operator must ensure that the VOI information passed to the intercept team accurately reflects all information held on the detected vehicle. This enables the intercept team to assess the threat level and plan accordingly in accordance with 'TENR'.

Power to stop

New Zealand legislation provides Police with various powers to stop vehicles. However, Police do not have a blanket power to stop any vehicle except for the purpose of a [compulsory breath test](#). As a general rule:

- For alerts relating to the [Land Transport Act 1998](#) offences, section 114 applies.
- For alerts where the [Search & Surveillance Act 2012](#) applies, refer to sections 9 and 121.

Some NIA VOI alerts such as 'other' will require the ANPR officer to check the alert text to determine if a power to stop exists. For more information refer to:

- 'New Zealand Bill of Rights'
- 'Traffic patrol techniques'
- 'Perimeter control'.

VOI alert - intercept team

Once notified of the alert type and vehicle description, the intercept team can prepare to stop the vehicle. Depending on the alert type consider:

- the statutory obligations pursuant to the power to stop under the [Search & Surveillance Act 2012](#);
- the risk the driver may fail to stop; and
- the risk the driver or passengers may flee on foot.

For more information on stopping vehicles refer to: '[Traffic patrol techniques](#)'.

If a vehicle fails to stop, follow the '[Fleeing driver policy](#)' and '[Urgent duty driving](#)' policies. Intercept staff should be aware that a VOI, failing to stop on request, does not automatically provide sufficient grounds to pursue the fleeing vehicle.

Approaching the driver

For information on approaching the driver of a vehicle refer to: '[Traffic patrol techniques](#)'.

Acting on the alert

Remember that some VOIs may no longer be of interest to Police but are yet to be expired. This must be considered when dealing with the driver.

For information on actions to be taken when acting on the alert refer to the appropriate Police Manual chapter. The main chapters are listed below:

- '[Alcohol and drug impaired driving](#)'
- '[Arrest and detention](#)'
- '[Driver licensing](#)'
- '[Impounding vehicles](#)'
- '[Issuing non operation orders](#)'
- '[Motor vehicle offences](#)'
- '[Motor vehicle registration and licensing](#)'
- '[Motor vehicle noise enforcement](#)'
- '[Offence notices](#)'.

Following the stop

If it is necessary to do so, update or expire the NIA alert to reflect the current status of the vehicle or notify the agency responsible for the source data. Ensure that intelligence notings are submitted in a timely manner.

Access to and retention of ANPR data

VOI data entered into ANPR

VOI data consists of vehicle registration numbers which are of interest to Police or require enforcement action, eg, high risk drivers. As the VOI data is derived from different data sources it must be treated the same as NIA data in accordance with the policies and rules set out in the [NIA manual](#).

District intelligence units and operational groups are authorised to create NIA alerts, by linking high risk drivers or offenders to vehicles, in order to target specific problems.

NIA is under utilised currently for the detection of POIs / VOIs, such as:

- High risk drivers,
- POIs with warrants to arrest, and
- POIs wanted for breach of bail.

By improving the linking of POIs to vehicles, improved detection and apprehension of POIs can be achieved for both ANPR, and during mobile QVRs.

Note: An appropriate expiry date must be entered against the alert in NIA.

Regardless of the alert entered onto NIA, expiry dates are critical to effective use of the ANPR vehicle and mobile queries. This is important as a POI may drive several vehicles. District intelligence units and operational groups must not create their own databases for use with ANPR.

VOI alerts which trigger the automated VOI extract file for ANPR are currently:

- Known to be driven by a disqualified driver
- Known to be driven under the influence of Drugs or Alcohol
- Driver Forbidden to Drive
- Non Op Order Pink Sticker
- Non Op Order Green Sticker
- Prohibition Notice s.248 LTA issued
- Wrecked i.e. plates removed from vehicle for disposal
- Stolen vehicle alert
- Petrol Drive Off
- Other (specify boy racer events)
- Person Safety Alert
- Organisation Safety Alert
- Sought
- Important Information.

VOI data from other Government agencies, eg, the New Zealand Transport Agency, may also be utilised in the ANPR system. This must only be data from agencies that have a written agreement with Police to share data for the purposes of ANPR deployments.

Data obtained from ANPR deployments

Data obtained from deployments will only be retained for 48 hours.

The data obtained from ANPR deployments consists of:

- a list of registrations captured by the ANPR camera;

- an image of a registration plate; and
- an image of part or all of the vehicle (depending on how the camera is set up).

At the end of every shift, the ANPR operator must:

- upload data from the ANPR system to a secure USB flash drive ('Ironkey'); and
- on return to their Police station, transfer the data to the BOSS system. The data may be manually processed and deleted, or the BOSS system will automatically delete the data after 48 hours.

All ANPR data retained for processing must only be stored in the J:Drive, ANPROVI folder, Endshift folder, and into your respective districts folder. If records are in excess of 48 hours old and the software is activated, the system will automatically delete the data.

If you have access to BOSS Server, download the Iron Key directly onto the standalone BOSS laptop by completing a synchronisation.

The data will be of no use if it is processed after 48 hours from the time the read or hit was obtained, as BOSS automatically deletes the information after this period.

Conditions of use

The underlying principle governing the proper use of the ANPR database is it must be used for Police business purposes only. Refer to the information on Police computers section in the '[Information security](#)' part of the 'Information management, privacy and assurance' chapter in the Police Manual chapter.

Removal of ANPR data from database

All data obtained from ANPR deployments automatically drops off the BOSS system after 48 hours.

Privacy Act implications

Collection of personal information (number plates) using ANPR has implications under the Privacy Act 2020. To ensure Privacy Act compliance, it is important that the procedures in these instructions are followed. In particular:

- ANPR must only be used where it is necessary for a lawful purpose connected to a Police function. In this case, the purpose is identification of high risk drivers and offenders to enhance enforcement opportunities.
- The information that is collected must be stored securely, and not retained for longer than necessary.

ANPR data from the database must not be circulated or disclosed to any other Government or third party organisation or person without the express authorisation from the Commissioner, or another officer delegated by the Commissioner to give such authorisation.

Examples of proper use of the ANPR database

ANPR data may be used as an investigative tool for the purposes listed in this table. The table also provides examples of proper use.

Purpose	Example of proper use
Locate an offender	A constable may stop a vehicle that is linked to an offender requiring further Police action.
Locate lost or stolen vehicles	<ul style="list-style-type: none"> • A vehicle is reported stolen and Police create an alert in NIA. • A vehicle identified as part of a deployment may be stopped; or • a constable could check the previous 48 hours of ANPR deployment records to determine if the vehicle's movements can be determined to assist in its location and recovery.
High risk drivers	A constable may intercept a vehicle that is linked to a high risk driver, ie, recidivist drink driver or person with a warrant to arrest.

Examples of improper use of the ANPR database

ANPR data must be used in connection with a lawful Police activity. Using data in the absence of a law enforcement purpose will constitute a breach of the [Privacy Act 2020](#).

ANPR data should not be used...	Example of improper use
in situations where Police attend peaceful protests or meetings where members of the public are exercising their right to freedom of expression.	A constable is supervising a peaceful public meeting. S/he uses the ANPR camera to record the registration numbers of all the vehicles travelling to the venue. S/he knows the vehicles are unlikely to be VOIs but plans to check the captured number plates in NIA to determine the names and addresses of the meeting attendees.
to monitor the movements of a person in the absence of any suspected unlawful activity.	A constable observes a person they would like to meet socially driving a vehicle and makes a note of the vehicle's registration plate. The constable checks the ANPR database to determine the vehicle's movements in the hope of being able to meet that person.
for the purposes of political, commercial, or financial gain.	In addition to being a Police employee, a constable owns a business with her/his partner. The constable learns that a representative of a rival company is in the local area. S/he knows the details of the vehicle the representative is driving and checks the ANPR database to monitor the movements of that vehicle.

If a Police employee is uncertain whether ANPR data is being used legitimately, they must discuss the matter with their supervisor.

Version number: 8

Owner: NM: Criminal Investigations

Publication date: 27/04/2016

Last modified: 01/12/2020

Review date: 26/10/2021

Printed on : 16/12/2020

Printed from : http://tenone.police.govt.nz/pi/automatic_number_plate_recognition

NEW ZEALAND POLICE

AND

AUROR LIMITED

Auror.



AGREEMENT dated 13 August 2018

PARTIES

- (1) **THE SOVEREIGN IN RIGHT OF NEW ZEALAND** acting by and through the Commissioner of Police ("**Police**")
- (2) **AUROR LIMITED** of 32 Nikau Street, Eden Terrace, Auckland 2021 ("**Auror**")

BACKGROUND

- A Auror has developed a crime intelligence platform that helps Police and the community work together to prevent and solve crime [REDACTED]. Auror will provide Businesses and Police with access to the Auror Platform for the purposes of reporting, informing, preventing, and reducing crime.
- B The purpose of this Agreement is to:
- Share information amongst Businesses and with Police to prevent crime and reduce victimisation.
 - [REDACTED].
 - Empower Businesses to prevent crime.
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - Enhance community safety outcomes.
- C This Agreement sets out the terms upon which Auror will make available the Platform and provide the Services to Police and comprises the following Commercial Terms and the Standard Terms and Conditions set out in Schedule 1.

Commercial Terms

Customer	New Zealand Police
Commencement Date	
Initial Term	
Renewal Term	Police may extend the term of this Agreement for by mutual agreement with Auror in writing (<i>Renewal Term</i>), such agreement not to be unreasonably withheld.
Territory	New Zealand
Platform Functionality	<div></div> <ul style="list-style-type: none"><div></div>Ability for Businesses to share information to prevent crime.<div></div><div></div><div></div> <div></div>
Police Support	Police will provide the following assistance to Auror: <ul style="list-style-type: none">Allow for the online reporting of retail crimes from Businesses to Police via the Platform.<div></div><div></div><div></div>Provide an Executive sponsor to meet with Auror quarterlyAs appropriate make decisions and give approvals reasonably required by Auror to enable delivery of this Agreement. Police will use reasonable efforts to make or give all decisions and approvals within reasonable timeframes.
Fees	<div>Platform Access Fee:</div> <div></div> <div></div> <div></div> <div></div>

	<div style="background-color: black; width: 100%; height: 20px;"></div>
Support	<p>Auror will provide <div style="background-color: black; width: 100%; height: 15px;"></div></p> <div style="background-color: black; width: 100%; height: 30px;"></div> <p>Support phone: <div style="background-color: black; width: 50px; height: 15px;"></div></p> <p>Support email address: <div style="background-color: black; width: 80px; height: 15px;"></div></p> <div style="background-color: black; width: 100%; height: 20px;"></div>
Key Contacts	<p>Auror:</p> <p>Key Contact Person: <div style="background-color: black; width: 150px; height: 15px;"></div></p> <p>Administration and Invoicing: <div style="background-color: black; width: 60px; height: 15px;"></div></p> <p>Support and Technical Assistance: <div style="background-color: black; width: 80px; height: 15px;"></div></p> <hr/> <p>Police:</p> <p>Key Contact Person: <div style="background-color: black; width: 150px; height: 15px;"></div></p> <div style="background-color: black; width: 100%; height: 20px;"></div> <div style="background-color: black; width: 100%; height: 20px;"></div>

SIGNED

<p>For THE SOVEREIGN IN RIGHT OF NEW ZEALAND acting by and through the COMMISSIONER OF POLICE or his or her authorised delegate:</p>	
Signature:	<div style="background-color: black; width: 100%; height: 30px;"></div>
Name:	<div style="background-color: black; width: 100%; height: 20px;"></div>
Position:	<div style="background-color: black; width: 100%; height: 20px;"></div>
Date:	<div style="background-color: black; width: 100%; height: 20px;"></div>

<p>For AUROR LIMITED:</p>	
Signature:	<div style="background-color: black; width: 100%; height: 30px;"></div>
Name:	<div style="background-color: black; width: 100%; height: 20px;"></div>
Position:	<div style="background-color: black; width: 100%; height: 20px;"></div>
Date:	<div style="background-color: black; width: 100%; height: 20px;"></div>

SCHEDULE 1 – STANDARD TERMS & CONDITIONS

It is agreed as follows.

1 Contract Administration

- (a) In the event of a conflict, inconsistency or ambiguity between any provisions or parts of this Agreement, the provisions will prevail in the following decreasing order of precedence:
- (i) the provisions of the Commercial Terms; and
 - (ii) the remaining provisions of this Agreement.

2 General Conduct

Both parties agree to:

- (a) act in good faith and demonstrate honesty, integrity, openness and accountability in their dealings with each other;
- (b) discuss matters affecting this Agreement or the delivery of the Services, whenever necessary;
- (c) notify each other immediately of any actual or anticipated issues that could:
 - (i) significantly impact on the Services or the Charges; or
 - (ii) receive media attention;
- (d) be responsible for the actions of its Personnel and ensure that Personnel adhere to the terms of this Agreement;
- (e) record any changes to this Agreement in writing and be signed by both parties, which may be executed through an exchange of emails where the authors have delegated authority to approve.
- (f) not publicly display (including posting on websites or social networking sites) objectionable or derogatory comments about the services provided under this Agreement, this Agreement, or each other, and to ensure that its Personnel do not do so; and
- (g) comply with all applicable laws and regulations.

3 Access to Platform

- (a) [REDACTED]
- (b) Auror will provide Police with login credentials for each User.
- (c) Auror must respond promptly, accurately and adequately within reason to any request for information made by Police in relation to this Agreement, including for the purpose of enabling Police to comply with its internal and external reporting and accountability obligations.
- (d) Auror must create and maintain full, accurate and accessible records relating to the provision of the Services and the Charges charged under this Agreement, to the standards required under the Public Records Act 2005.
- (e) [REDACTED]
- (f) Police must not, and must procure that each User must not, access the Platform using login credentials that have not been specifically allocated to the Registered User by Auror to Police.
- (g) Police must, except as required by law, maintain the confidentiality of all login information and must immediately notify Auror of any suspected or actual unauthorised use of the login credentials.
- (h) Police is responsible for any and all activities that occur under Police's account(s) for the Platform, whether or not authorised by Police, including any action or inaction taken as a result of information provided via the Platform.
- (i) Audit:
- (i) At Police's request, Auror must allow Police (or an independent auditor nominated by Police) to conduct audits of Auror's compliance with this Agreement.
 - (ii) Without limiting clause 3(j)(i), Auror must co-operate in a timely manner in relation to any audit undertaken in accordance with this clause 3(j), including promptly providing Police or the auditor (as the case may be) with reasonable access and assistance in respect of any audit, including reasonable access to Auror, its Personnel, and the facilities, records and resources which are owned by Auror and used in the provision of the Platform and the Services.
 - (iii) Police or the auditor (as the case may be) may make copies of any records or other information acquired by it for the purposes of any audit undertaken in accordance with this clause 3(j).
- (j) Auror is an independent contractor to Police and is not an employee of Police.
- (k) Auror must not enter into any agreement or arrangement that will, or is likely to:
- (i) prejudice Auror's ability to meet its obligations under this Agreement; or
 - (ii) create a conflict of interest for Auror.

4 Registered Users

(a) Only Registered Users may access and use the Platform.

(b) Police may request that Auror add, replace or remove Police Registered Users by written notice to Auror. [REDACTED]

(c) [REDACTED]

5 Auror Materials

(a) (ownership) [REDACTED]

(b) (licence) Auror grants to Police a non-transferable and non-exclusive licence in the Territory for the Term to use the Auror Materials for the Permitted Purpose.

(c) [REDACTED]

6 Use of Auror Materials

Police must, and must procure that its Police Registered Users must:

(a) not use the Auror Materials for any unlawful purpose;

(b) not sell, grant a sub-licence of, or reproduce, the Auror Materials without Auror's prior written consent;

(c) not copy the Auror Materials except where such copying is incidental to the normal use of the Platform for the Permitted Purpose;

(d) not use the Platform in a way that could damage, disable, overburden, impair or compromise Auror's systems or security or interfere with other Registered Users;

(e) not, except as contemplated by this Agreement, collect or harvest any information or data, or attempt to decipher any transmissions to or from the Platform or services used by Auror; and

(f) not reverse disassemble, decompile or reverse engineer, or directly or indirectly allow or cause a third party to disassemble, decompile or reverse engineer the whole or any part of the Platform, or any locking or security device used or supplied with the Platform, or otherwise attempt or allow any other party to attempt to obtain the algorithms by which the Platform perform its functions.

7 Updates

8 Technical Assistance

(a) Auror may provide technical assistance and training services to Police Registered Users at its discretion and must provide the Support set out in the Commercial Terms.

(b) [REDACTED]

(c) Police will abide by the minimum technical and system requirements outlined by Auror, acting reasonably, and will be responsible for whitelisting any websites required for the Platform to function.

9 Intellectual Property Rights

9.1 Brand Marks

(a) (ownership) [REDACTED]

(b) (licence) Each party (the "first party") grants to the other party a non-transferable and non-exclusive licence in the Territory for the Term to use the first party's Brand Marks for the purposes of performing its obligations and exercising its rights under this Agreement.

(c) Auror may use Police's logo and name on the Website or the Platform marketing materials on agreement by both parties and in accordance with any Police brand guidelines notified by Police to Auror in writing from time to time provided Police approves the use of its logo and name in each case, such approval not to be unreasonably withheld. Auror may also use any testimonials provided by Police Registered Users.

(d) Police will provide reasonable assistance to Auror with case studies regarding Police's involvement with Auror and successful uses of the Platform, including with other law enforcement agencies.

(e) Public references to this Agreement and the relationship between Auror and Police will be undertaken using the word "Partnership" or "Partner".

9.2 Auror warrants that the Platform, the Services and the Auror Materials and Police's use of them in accordance with this Agreement will not infringe the Intellectual Property Rights of any third party.

10 Privacy

- (a) Each of Auror and Police must comply with the Privacy Act and any other applicable Privacy Laws, in respect of any Personal Information that:
- (i) one party discloses to the other party; or
 - (ii) comes into the possession or control of a party by any means, including through the use of the Platform.
- (b) If Police becomes aware during the Term that any data is inaccurate or out of date, it must use all reasonable endeavours to notify Auror or update that data on the Platform.
- (c) Auror must not transfer Police Data outside New Zealand except with the prior written consent of Police. Any transfer of Police Data outside of New Zealand must be in accordance with the Privacy Act.
- (d) As at the date of this Agreement, Auror is [REDACTED], which complies with the Privacy Act.

11 Confidential Information

- (a) Subject to clause 11(b), a party must not disclose, or use for a purpose other than as contemplated by this Agreement, information that:
- (i) is by its nature confidential;
 - (ii) is marked by either party as 'confidential', 'in confidence', 'restricted' or 'commercial in confidence';
 - (iii) is provided by either party or a third party 'in confidence';
 - (iv) either party knows or ought to know is confidential, or
 - (v) is of a sensitive nature or commercially sensitive to either party.
- (b) Each party confirms that it has adequate security measures to safeguard the other party's Confidential Information from unauthorised access or use by third parties, and that it will not use or disclose the other party's Confidential Information to any person or organisation other than:
- (i) to the extent that use or disclosure is necessary for the purposes of providing the services or in the case of Police using the Services;
 - (ii) if the other party gives prior written approval to the use or disclosure;
 - (iii) if the use or disclosure is required by law (including under the Official Information Act 1982), Ministers or parliamentary convention; or
 - (iv) if the information has already become public, other than through a breach of the obligation of confidentiality by one of the parties.

12 Termination

- (a) **(for cause)** Subject to clause 12(b), either party may terminate this Agreement with immediate effect by giving written notice to the other party at any time if the other party breaches any warranty or any other provision of this Agreement which is incapable of being remedied, or where the breach is capable of being remedied, but the party fails to remedy the breach within [REDACTED]
- (b) **(termination for failure to comply with restrictions)** Without limiting clause 12.1(a), Auror may [REDACTED]
- (c) [REDACTED]

13 Consequences of termination

- (a) On termination of this Agreement for any reason, Police will lose all right to use the Auror Materials, and must immediately delete all copies of the Platform, discontinue (and procure that Registered Users discontinue) using and accessing the Auror Materials and return to Auror any Associated Documentation supplied under this Agreement.
- (b) On Auror's request, Police must procure one of its officers to certify to Auror that all copies of the Auror Materials have been returned, deleted or destroyed as required under this clause.
- (c) Police must, [REDACTED] pay to Auror any fees incurred and/or owing under the Agreement up to and including the date of termination or expiry except to the extent the payment is disputed in accordance with clause 16.1(b).

14 Accrued rights and remedies and survival

Termination or expiry of this Agreement does not affect the rights and obligations of the parties accrued up to and including the date of termination. Without limiting any other provision of this Agreement, clauses 5 (Use of Auror Materials), 9 (Intellectual Property Rights), 10 (Privacy), 11 (Consequences of termination), this clause 14 (Accrued rights and remedies and survival), 15 (Disclaimer), and any other clauses which should by their nature survive termination of this agreement, survive termination or expiration of this Agreement for any reason.

15 Auror Personnel

Auror will:

- (a) comply with the Standards of Integrity and Conduct issued by the State Services Commission (see www.ssc.govt.nz) and any other relevant codes of conduct notified by Police to Auror from time to time;
- (b) must ensure that all its Personnel comply with the terms of this Agreement; and
- (c) not employ any person or contractor to perform its obligations under this Agreement who is not prepared to undergo and pass a security check by Police or to Police's reasonable satisfaction.

16 Dispute Resolution

16.1 Resolving disputes

The parties agree to use their best endeavours to resolve any dispute or difference that may arise under this Agreement.

- (a) The following process will apply to disputes:
 - (i) a party must notify the other if it considers a matter is in dispute.
 - (ii) the Contract Managers will attempt to resolve the dispute through direct negotiation
 - (iii) if the Contract Managers have not resolved the dispute within 10 Business Days of notification, they will refer it to the parties' senior managers for resolution, and
 - (iv) if the senior managers have not resolved the dispute within 10 Business Days of it being referred to them, the parties shall refer the dispute to mediation or some other form of alternative dispute resolution.
- (b) **Dispute over invoice**
 - (i) If Police disputes in good faith the whole or any portion of any Valid Tax Invoice, Police will pay the portion of the Valid Tax Invoice that is not in dispute, but may withhold payment of the disputed portion until the dispute is resolved following the procedure set out in clause 16.1.
 - (ii) Police will provide Auror with reasons for its dispute of the Invoice (or part thereof) and such notification shall serve as a notice of dispute,
- (c) If a dispute is referred to mediation, the mediation will be conducted:
 - (i) by a single mediator agreed by the parties or if they cannot agree, appointed by the Chair of the Resolution Institute.
 - (ii) on the terms of the Resolution Institute standard mediation agreement or rules, as applicable, and
 - (iii) at a fee to be agreed by the parties or if they cannot agree, at a fee determined by the Chair of the Resolution Institute.
- (d) Each party will pay its own costs of mediation or alternative dispute resolution under this clause 16.

16.2 Obligations during a dispute

- (a) If there is a dispute, each party will continue to perform its obligations under this Agreement as far as practical given the nature of the dispute.

16.3 Taking court action

- (a) Each party agrees not to start any court action in relation to a dispute until it has complied with the process described in clause 16.1, unless court action is necessary to preserve a party's rights.

17 Disclaimer

Police agrees and acknowledges that, to the extent permitted by Law, Auror:

- (a) [REDACTED]
- (b) [REDACTED]
- (c) [REDACTED]

18 Limitation of liability

- (a) [REDACTED]
- (b) To the maximum extent permitted by law, the maximum total liability of Police under or in connection with this Agreement whether arising in contract, tort (including negligence) or otherwise is the total amount which would be payable under this Agreement if all Services had been provided in accordance with this Agreement, with the exception of breach of Confidential Information which has unlimited liability.
- (c) To the maximum extent permitted by law, the maximum total liability of Auror under or in connection with this Agreement whether arising in contract, tort (including negligence) or otherwise is the total amount which would be payable under this Agreement if all Services had

been provided in accordance with this Agreement, with the exception of breach of Confidential Information and breach of Intellectual Property [REDACTED]

19 Assignment

- (a) Auror may transfer, assign, charge, sub-contract or otherwise deal with an Agreement, or any of its rights or obligations arising under it, at any time during the term of the Agreement provided it has Police's written consent, such consent not to be unreasonably withheld.

20 General

- (a) **(Amendment)** This Agreement may be amended only by another agreement executed by all the parties.
- (b) **(Waiver)** No failure to exercise or delay in exercising any right, power or remedy under this Agreement operates as a waiver. A single or partial exercise or waiver of the exercise of any right, power or remedy does not preclude any other or further exercise of that or any other right, power or remedy. A waiver is not valid or binding on the party granting that waiver unless made in writing.
- (c) **(Remedies cumulative)** The rights, powers and remedies provided to a party in this Agreement are in addition to, and do not exclude or limit, any right, power or remedy provided by law or equity or any agreement.
- (d) **(Severability)** Any provision of this Agreement which is prohibited or unenforceable in any jurisdiction is ineffective as to that jurisdiction to the extent of the prohibition or unenforceability. That does not invalidate the remaining provisions of this Agreement nor affect the validity or enforceability of that provision in any other jurisdiction.
- (e) **(Notices)** Any notice to be given under this Agreement must be in writing and hand delivered or sent by email or post to the parties' respective addresses as set out in the Commercial Terms under Key Contacts. Any notice is deemed to be received:
- (i) if personally delivered, when delivered;
 - (ii) if posted, three Business Days after posting; or
 - (iii) if sent by email, one hour after sending. If the notice is a notice of termination, a copy of that email must be immediately personally delivered to the Chief Executive or equivalent officer of the other party at the other party's last known physical address.
 - (iv) Any notice received after 5pm or on a day which is not a Business Day is deemed not to have been received until the next Business Day.

21 Definitions and Interpretation

21.1 Definitions

The following definitions apply unless the context requires otherwise.

Associated Documentation means the documentation and/or other guides and printed materials made available to Police by Auror from time to time for the Permitted Purpose.

Auror Marks means the brands, trademarks, designs, logos or names of Auror.

Auror Materials means the Platform and the Associated Documentation.

Brand Marks means Auror Marks or Police Marks, as applicable.

Business Day means a weekday on which banks are open in Auckland, New Zealand.

Businesses means [REDACTED]

Business Registered Users means [REDACTED]

Charges means the fees set out in the Commercial Terms.

Claim means, in relation to a party, a demand, claim, action or proceeding made or brought by or against the party, however arising and whether present, unascertained, immediate, future or contingent.

Confidential Information means all information of a confidential nature, in any form whether tangible or not and whether visible or not, disclosed or communicated by a party to the other, or learnt or accessed by, or to which the other party is exposed as a result of entering into this Agreement and includes, without limitation, any information and material concerning the contractual or commercial dealings, financial details, products or services (current or proposed) of Police, employees, internal policy, the Intellectual Property Rights of a party or dealings under this Agreement, and includes the Police Data.

Consequential Loss means any:

- (a) loss of profits, loss of revenue, loss of data, loss of or damage to reputation, loss of or damage to goodwill, loss of business opportunities (including opportunities to enter into or complete arrangements with third parties), loss of management time, damage to credit rating, or loss of business; and
- (b) any loss, not arising naturally (that is according to the usual course of things), from the relevant breach, whether or not such loss is reasonably supposed to have been in the contemplation of both parties, at the time they made the Agreement, as the probable result of the relevant breach.

Data means any data [REDACTED] Data does not include Police Data.

Feedback means any feedback provided by Police to Auror, including suggestions, ideas, information, comments, process descriptions or other information.

Intellectual Property Rights means all industrial and intellectual property rights of any kind including but not limited to copyright (including rights in computer software), trade mark, service mark, design, patent, trade secret, semi-conductor or circuit layout rights, trade, business, domain or company names, moral rights, rights in Confidential Information, know how or other proprietary rights (whether or not any of

these are registered and including any application, or right to apply, for registration) and all rights or forms of protection of a similar nature or having equivalent or similar effect to any of these which may subsist anywhere in the world.

Law means all laws including rules of common law, principles of equity, statutes, regulations, proclamations, ordinances, by-laws, rules, regulatory principles, requirements and determinations, mandatory codes of conduct, writs, orders, injunctions and judgments.

Loss means any claim, loss liability, cost or expense (including legal expenses on a full indemnity basis).

Permitted Purpose means [REDACTED]

Personal Information means "personal information" as defined in the Privacy Act and any other information relating to individuals that is subject to the operation of the Privacy Laws that either party has collected, received or otherwise has access to in connection with this Agreement.

Personnel means in respect of a person any employee, contractor, servant, agent, or other person under the person's direct or indirect control and includes any sub-contractors.

Platform means [REDACTED]

Police Data means all information relating to Police, its business strategies, marketing plans, facilities, systems, technologies, and Police personnel's data such as names, QIDs (logons) etc. that can be used when completing the National User Reports.

Police Marks means the brands, trademarks, designs, logos or names of Police

Privacy Act means the *Privacy Act 1993*.

Privacy Law means:

- (a) the Privacy Act and its related Information Privacy Principles;
- (b) any applicable legislation from time to time in force affecting privacy, personal information or the collection, handling, storage, processing, use or disclosure of personal data; and
- (c) any ancillary rules, guidelines, orders, directions, directives, codes of conduct or other instruments made or issued by a Government Agency under an instrument identified in paragraphs (a), (b) or (c),

as amended from time to time.

Police Registered User means [REDACTED]

Registered Users means [REDACTED]

Services means the services described in this Agreement to be provided by Auror.

Term means the Initial Term and, where applicable, any applicable Renewal Term.

Territory means the territory or territories set out in the Commercial Terms.

Update means any update or upgrade to the Auror Materials issued by Auror from time to time.

Website means the website at the domain www.auror.co or any other website owned or operated by Auror, and includes any mobile/tablet versions of that website and any mobile/tablet or desktop applications.

BUSINESS CASE:
Purchase of an Automatic Number Plate Recognition (ANPR) software database to receive ANPR data from existing 3rd party ANPR sites in the Counties Manukau District.
COVER SHEET

☒ [Copy and paste this tick into the appropriate places]

REFERENCE	District Command Centre
TOPIC	Design and purchase of ANPR database software for the Counties Manukau District Command Centre
SPONSOR	s.9(2)(a) OIA
PREPARED BY	Senior Constable s.9(2)(a) OIA
DATE SUBMITTED	14 June 2016

DISTRIBUTION

☒ General Manager Finance
 Full Police Executive Committee
 PEC Resource Management subcommittee
☒ Other: District Commander approval

URGENCY

☒ Urgent
 Semi-urgent
 Not urgent

ACTION REQUIRED

Information only Formal noting ☒ Recommendations for decision

DETAILS OF FUNDING REQUEST

☒ Bid included in this year's approved capex programme
 No previous bid – request for reserve funding
☒ Other: Funding from District Sources

IMPLICATIONS

☒ Financial resources
 Legislative
 Maori or Pacific People
 Human resources
 Policy
☒ Organisational Performance
 EEO/OSH
 Training
☒ Public relations/communications
 Other: Staff safety implications and policy compliance

CONSULTATION

Human Resources
 Organisational Performance Group
 Strategic Policy Group
☒ Policing Development Group
 Cultural Affairs
 Training Service Centre
☒ Information & Technology
 Corporate Communications
☒ Other:
 National Finance Manager

BUSINESS CASES \$25,000 AND OVER

TOPIC: Purchase of ANPR database software to allow the Counties Manukau DCC to connect to and partner with multiple existing ANPR sites within the District.

SPONSOR: s.9(2)(a) OIA

1. Proposal

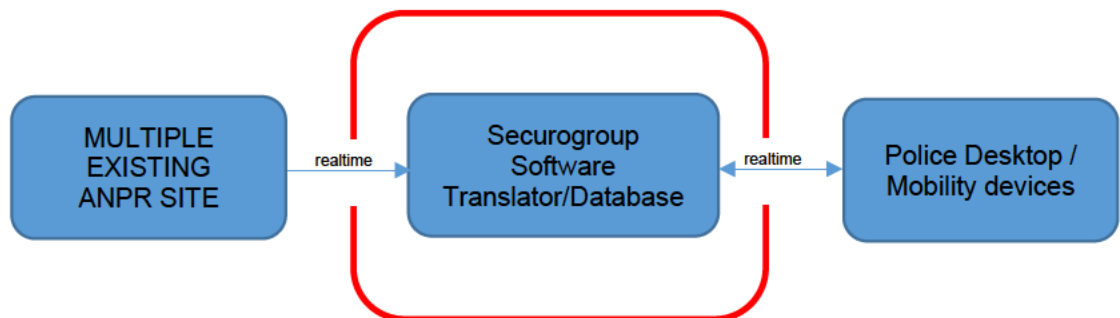
- 1.1 This proposal seeks funding for further software development for the Securogroup Software currently installed in the DCC. The additional development will enable real-time processing of ANPR data from multiple existing 3rd party ANPR sites within the Counties Manukau District.
- 1.2 The core function of the software would provide a single database for the receipt of 24/7 real-time vehicle plate data from all the existing (and future) dedicated ANPR sites in the Counties Manukau Police District. These sites currently include s.6(c) OIA
- 1.3 Accessibility to this software will continue to be restricted s.6(c) OIA within Police.
- 1.4 Although this is a Counties Manukau project, the foundation of the software design has allowed for this ANPR solution to be rolled out nationally, should future demands require it.

2. Background

- 2.1 Out of scope

- 2.2 Throughout the Counties Manukau District there are multiple existing dedicated ANPR camera sites. However these sites use a variety of ANPR products from a range of vendors. No software exists that will talk to these sites simultaneously and in real-time. s.6(c) OIA

This Business Case focuses on the development of software which will simultaneously connect to these multiple ANPR sites in real-time. This data will be processed against a current Vehicle of Interest (VOI) list and provide alerts/access via Enterprise and Mobility interfaces.


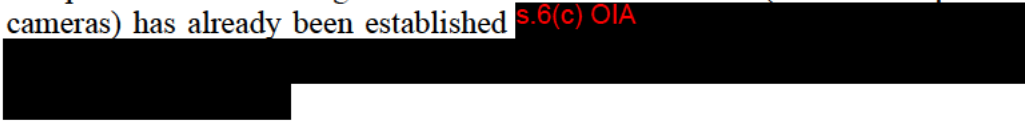


- 2.3 This real-time processing will enable immediate deployment by DCC, regardless of the specific ANPR system or location. This will greatly increase Police's ability to detect vehicles being used for criminal activity and provide a proven technology platform to apprehend VOI vehicles.
- 2.4 It is envisaged that upon implementation of this proposed desktop software, one further business case will be submitted to enable ANPR activation via an App on the Police mobility devices. s.9(2)(b) OIA

3. Requirements

3.1 ANPR Network Connection

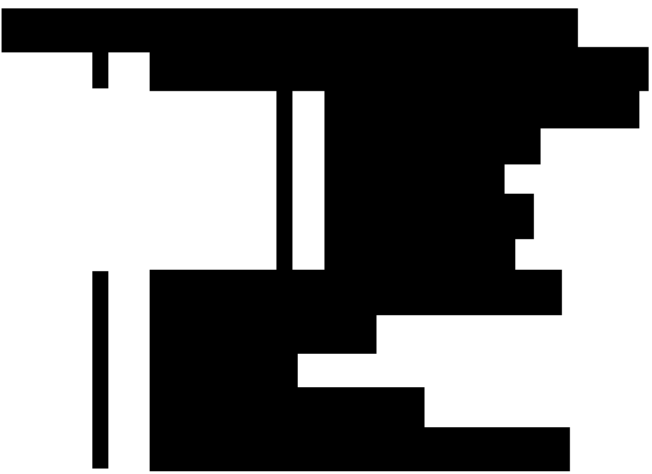

The process of connecting to these dedicated ANPR sites (and their respective cameras) has already been established s.6(c) OIA



3.2 ANPR Sites of Interest

There are a number of business entities within the District that currently connect, or intend to connect their ANPR to the DCC, should suitable software allow this connectivity.

s.6(c) OIA



3.3 Software functionality

A significant issue exists within Counties Manukau DCC, relating to our inability to partner with these existing ANPR sites. This issue has arisen due to the absence of computer/server/software to receive live data from these sites.

Police have identified three key roles that ANPR plays in Counties Manukau. Accordingly the software architecture and user interface has been designed around these areas.

1) ***Real-time deployment (DCC)***

VOI alerts will primarily be monitored and deployed via the live link in the DCC. s.6(c) OIA

2) ***Enquiry work (Criminal investigations)***

s.6(c) OIA

3) ***Intelligence (Data analysis)***

The software functionality required for this section is simply the ability to export larger quantities of data for analysis. From a Police point of view this area contains a significant number of privacy issues. This is being worked through by a separate work-stream. It is envisaged that there will only be 1 or 2 users in each district with this level of access, as there will be strict business and legal guidelines to be adhered to.

3.4 Privacy

ANPR has significant privacy considerations relating to these three key areas. It needs to be clearly stated that this Business Case is in-separately connected to the development of the privacy policies and business rules. Whilst this Business Case focusses on the practical Hardware/Software development required, it needs to be emphasised that no 'go live' status would be assigned this software until all Privacy issues are signed off.

Preliminary work has been undertaken concerning wider privacy aspects. If this business case is approved, a designated workstream will need to be formalised and outcomes defined.

3.5 Staffing requirements

In the first instance (ANPR - Phase I), the handling of real-time District ANPR data would be handled by the DCC in the Prevention environment. s.9(2)(g) OIA

[REDACTED]

When the UK Police set up ANPR as an “add-on”, this technology quickly became a mainstream Policing tool and became integrated into the Police strategy, policies and business processes.

3.6 Data Storage

s.6(c) OIA, s.9(2)(b) OIA
[REDACTED]

Storage would be hosted on Securogroup’s existing servers Out of scope
[REDACTED]

3.7 Data Retention protocol

Police will be hosting ANPR data on a secure Securogroup server. This provides a secure encrypted network that does not interface with the World Wide Web. Because we are being provided with ANPR data from outside agencies, we (Police) do not determine the length of retention of this information.

s.6(c) OIA
[REDACTED]
Vehicles that hold no criminal interest to Police will automatically be deleted after this period.

3.8 Data Ownership

Unlike Police generated ANPR data (ie from Police owned ANPR vehicles), the data stored within this proposed ANPR server software is simply a further copy of the data already existing on the servers of the owners of the ANPR site. Police do not intend to own this data, but by mutual and transparent partnership utilise it for the apprehension of criminals.

3.9 Data hosting

3.10 **Network Security**

This will be overseen by both the existing provided Securogroup and Police ICT networks. Security is a critical facet over-arching all architectural design considerations. Having this ANPR network within the parameters of Police network puts the full Police network security regime over the project.

4. Physical Works

As previously mentioned, network connectivity to these proposed ANPR sites already exists, in a physical form. The implementation of the developed software will utilise existing Police computers (hardware) and accessibility will be gained through a web user interface.

4.1 Partnerships

Significant opportunity exists to further develop key partnerships with owners of ANPR sites in Counties Manukau.

This Business Case focusses on further development of relationship with Securogroup that already exists at both a National and District level.

4.2 Scope of Works

No scope of works or product development timetable has been finalised at this stage, however early indication suggests a 3 – 4 month period before an operational software release.

5. Financial Implications

s.9(2)(b) OIA

5.1 Risks

The following risks are possible if this case is not favourably considered:

- Police will continue to be unable to utilise valuable real-time ANPR within the District.
- Vehicle crime offenders will continue to drive through existing ANPR sites with no Police detection.
- Police will be viewed in a poor light for failing to partner with District Agencies due to lack appropriate technology.
- Negative impact on Trust and Confidence within the community.

5.2 Opportunities

The following opportunities are identified if this case is approved:

- Provide real-time data of stolen vehicles mobile within the District.
- Lay a robust foundation for ongoing development ANPR integration with Police.
- Disrupt criminal activity by intelligence led intervention.

- Increased success in tackling criminality on the roads.
- Deny offenders the use of the roads and motorways.
- Provide investigation support for Police staff by providing a single searchable ANPR database via the Enterprise Computers
- Provide significant Police/Partnership opportunity

6. **Developing of Partnerships**

Great opportunity exists to utilise partner's assets and provide feedback to them relating to criminal activity at their sites.

The ANPR software implementation provides a single point of reference relating to ANPR information from multiple partner organisations. The access and collation of this information allows Police to strategically advise partners on future ANPR installations.

7. **Maori and Pacific Implications**

Not applicable.

8. **Legislative Obligation**

A separate workstream will continue to finalise policy relating privacy obligations and business rules/processes.

9. **Public Relations**

ANPR is a relatively new tool for criminal investigation and to date has only existed in the branch of Road Policing. s.9(2)(g) OIA

[Redacted]

10. **Consultation**

ICT

s.9(2)(g) OIA

[Redacted]

The project does not involve any local ICT components.

11. Recommendations

It is recommended that the District Commander:

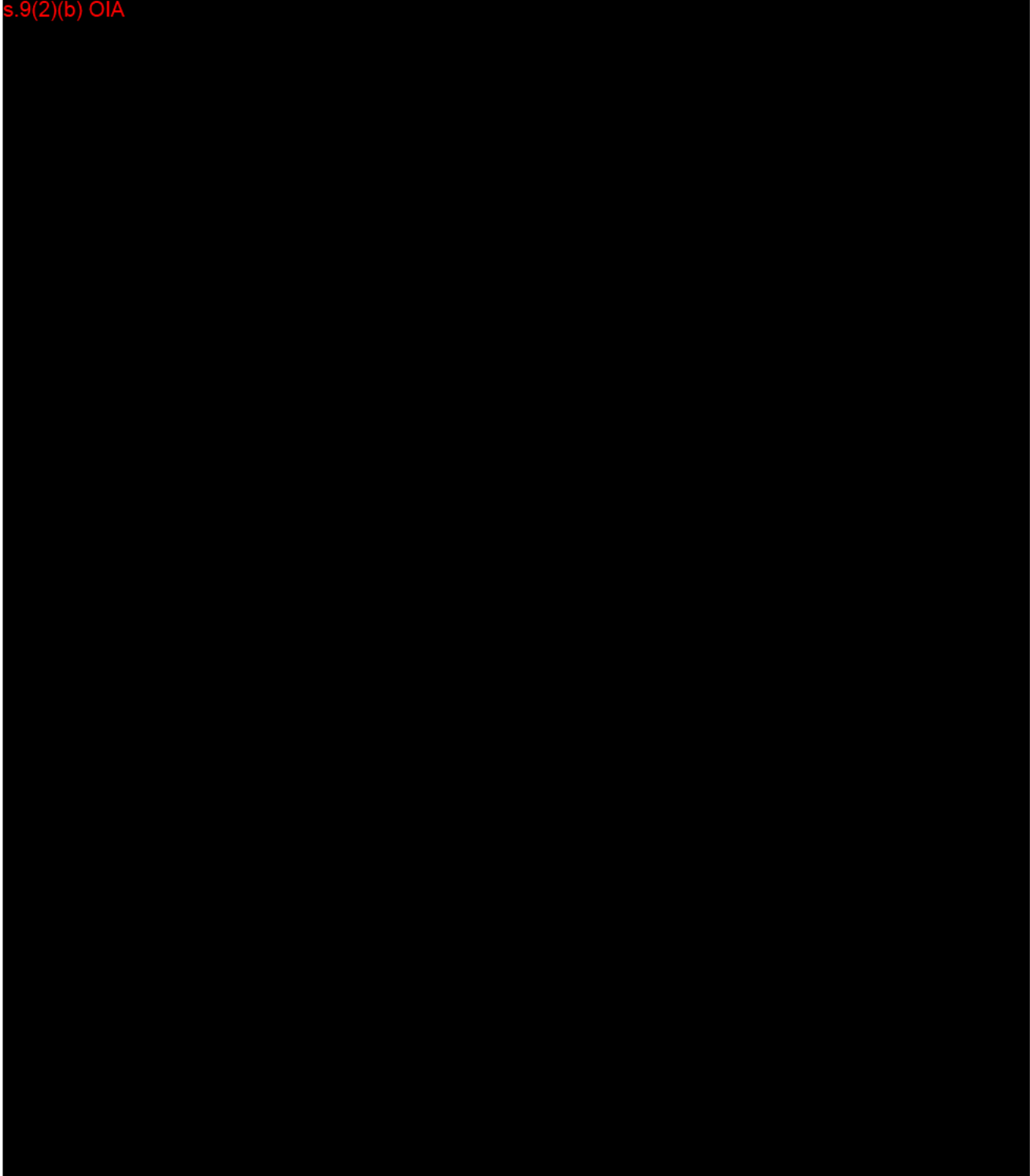
- (i) **Acknowledges** the potential organisational risks identified in this Business Case.
- (ii) **Confirms** that the mitigation of the risk can be achieved by the purchase and installation of the equipment and services outlined for the DCC either as a single purchase.
- (iii) **Notes** that the proposed installation carries significant opportunities for the reputation of the Counties Manukau Policing District.
- (iv) **Notes** that the proposed installation carries significant opportunities for the professionalism and investigative capability of Counties Manukau Staff.
- (v) **Approve** a one-off expenditure of s.9(2)(b) OIA from appropriate funds to purchase and installed as outlined.

Business case prepared by:
Senior Constable s.9(2)(a) OIA
CCTV Project Development
Policing Development Group

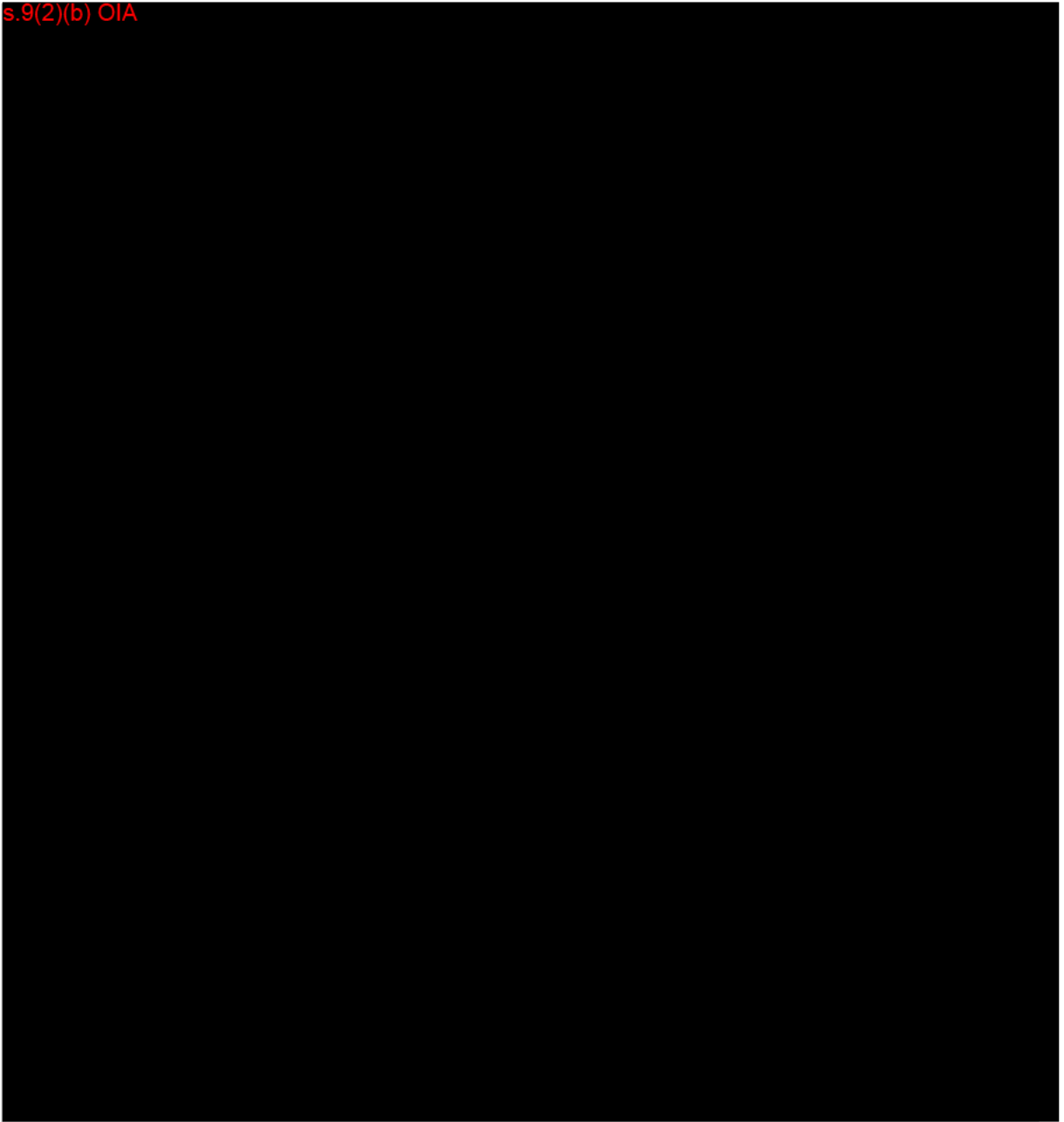
Business case sponsored by:
s.9(2)(a) OIA
Project Sponsor
Manager Policing Development Group

APPENDIX A (Software Design quote)

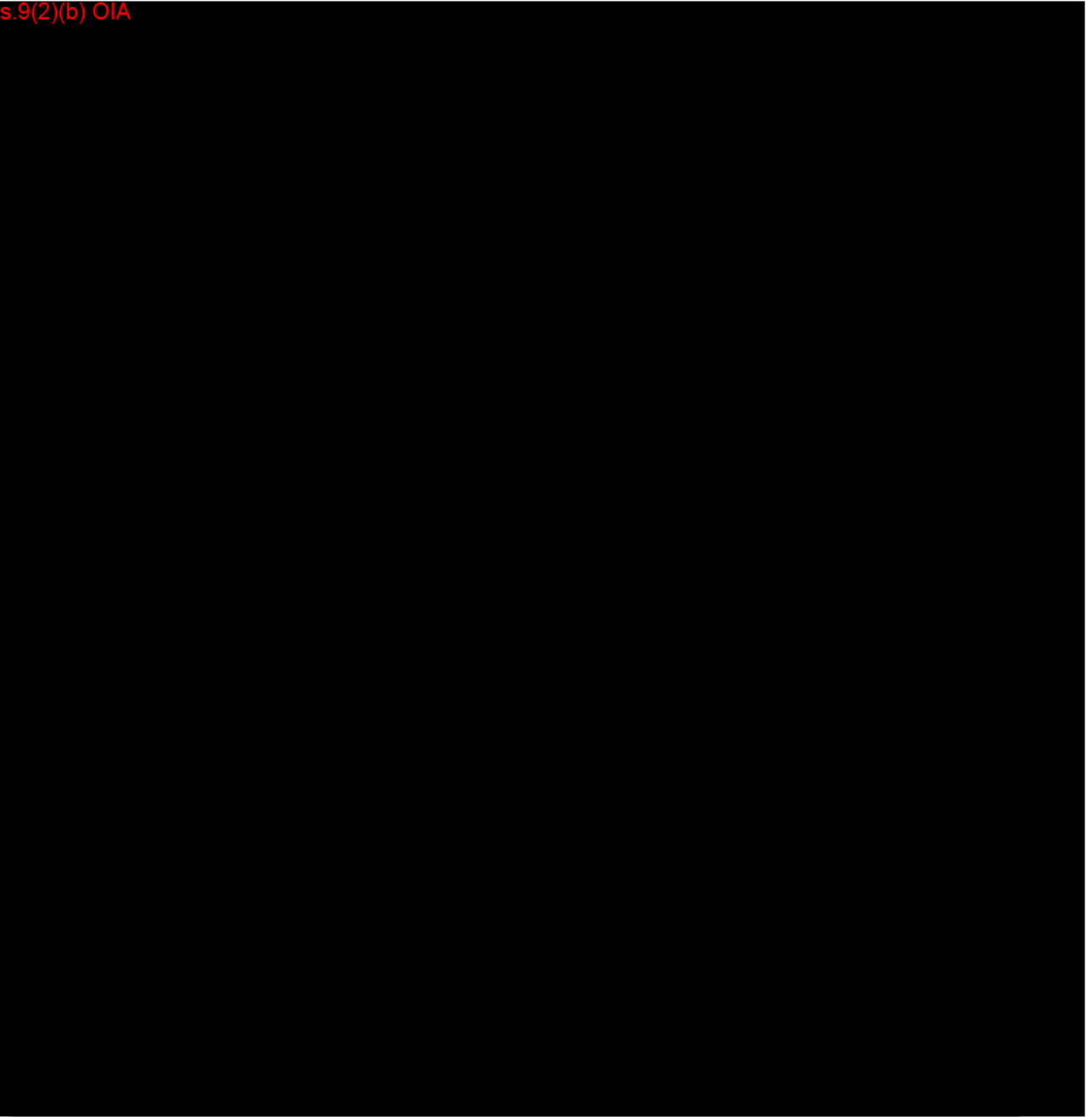
s.9(2)(b) OIA




s.9(2)(b) OIA



s.9(2)(b) OIA



s.9(2)(b) OIA



Annex A: ANPR operations - approved deployment models

Deployment name	Description	Minimum resources	Additional requirements
Limited scale deployments			
Carpark deployment	Mobile ANPR vehicle deployed to report stationary VOIs to an intercept officer, ie, stolen vehicles Location: Carparks and stationary vehicle gatherings. Purpose: Observe or intercept stationary VOIs.	ANPR operator and vehicle, intercept officer and support vehicle.	Nil.
Checkpoints			
ANPR Checkpoint	Static ANPR vehicle deployed to report mobile VOI activity to a static intercept team. Location: Areas where static checkpoints can be established. Purpose: Intercept mobile VOIs.	ANPR operator and vehicle, intercept officer and support vehicle.	Site plan, cones, and signage.
ANPR/TAG checkpoint	Static ANPR vehicle deployed to report mobile VOI activity to an intercept team adjacent to a TAG checkpoint. Location: With TAG checkpoints . Purpose: Intercept mobile VOIs and drink/drugged drivers.	ANPR operator and vehicle, intercept officer and support vehicle.	Co-ordinated site plan, TAG cones, and signage.
Multiple direction checkpoint	Single static ANPR vehicle deployed to report mobile VOI activity to a static intercept team from both directions. Location: Areas where static checkpoints can be established. Purpose: Intercept mobile VOIs from two directions	One ANPR operator and vehicle, sufficient intercept officers, and support vehicles.	Nil.
Mobile deployments			
Mobile ANPR	Static or mobile ANPR vehicle deployed to report or intercept mobile VOI activity Purpose: To intercept mobile VOIs	One ANPR operator/driver. Can be used single crewed, but vehicle must be stationary to read the alert.	Nil.
Non-standard deployments			
Mobile Interception	Static ANPR vehicle deployed to report mobile VOI activity to a mobile intercept team. Location: Areas where static checkpoints cannot reasonably be established. Purpose: Intercept mobile VOIs.	ANPR operator and vehicle, intercept officer, and support vehicle.	Site plan and pursuit mitigation plan.
Covert deployment	Activities and resources as approved by the National Manager: Road Policing on a case-by-case basis.		Written approval prior to deployment.



Introduction

- Body Worn Cameras (BWC) are an effective tool for police, providing important benefits that help prevent and resolve crime and make our staff and the public safer.
- BWC do have issues and risks, which can be mitigated with careful consideration.
- BWC are not beneficial unless they are complemented with an efficient and effective information management system, s. 9(2)(j) OIA
- New Zealand Police has been capturing footage of operating for over a decade (Tasercam), but do not use BWC currently. We do s. 9(2)(j) OIA manage an increasingly large amount of digital information.
- Should New Zealand police introduce BWC in the future, we are well placed to do so because we already have a tried, proven and functional digital information system to support BWC s. 9(2)(j) OIA .
- Capturing digital footage provides little benefit. The benefit is when the digital information has meaning or relevance. s. 9(2)(j) OIA
[REDACTED]
[REDACTED] having BWC without a 'backroom' system to achieve this would provide more risk than benefit.
- s.9(2)(g) OIA [REDACTED]

s. 9(2)(j) OIA

Body Worn Cameras (BWC) are widely used by law enforcement globally and within Australasia. Singapore police and most Australian states have either implemented BWC or are in the process of doing so. Most use the Axon camera and evidence.com system.

BWC is a system comprising two parts: hardware (the actual camera) and software (the system used to upload, store, analyse and manage footage, metadata, documents and stills).

The rise of digital information, either captured by police or supplied to police by the public, in the future provides both a risk and opportunity.

BWC are proving to be an effective tool for police officers and organisations. It provides preventative benefits (people behave differently when they know they are being filmed, less complaints), evidential benefits (by recording spontaneous admissions and earlier guilty pleas), safety benefits (less assaults on police) training and learning benefits (where officers can learn lessons from real events) and intelligence benefits (detailed offender associations can be better understood).

But they also have issues and risks, including cost (for hardware, software and storage), trust and confidence (recorded non-best practice police behaviour), security (of information, especially intelligence and evidential information), administration (official information demand) and most importantly, an inability to analyse the volume of information and provide meaningful information to staff to prevent crime.

New Zealand police have been using Taser cameras for over 10 years and have a very healthy partnership with Axon (Taser). s. 9(2)(j) OIA, s.9(2)(b) OIA

New Zealand police are very well placed to implement BWC in the future, s. 9(2)(j) OIA as it complements our processes and systems (beyond just the Taser device).

Background

BWC hardware (cameras) exist in a competitive marketplace. There are many different camera systems and they are decreasing in price over time. The camera is less important than the 'backroom' system that securely and efficiently stores that information.

The same cannot be said for the information management software required to effectively and efficiently manage high volumes of digital footage and data.

Axon's evidence.com is probably the best known software in the market place for such purposes, especially when directly paired with Tasers, Taser cameras and mobility devices.

s. 9(2)(j) OIA, s.9(2)(b) OIA

NZ Police is well placed to capture, store, share and dispose of digital information and evidence in the future.

There are established and effective processes operating, some legal precedents (at district court level only), well established OIA processes (through Ombudsman's investigation and decisions) and a well-established software platform to manage our current information to an evidential standard.

The key to being prepared for the potentially huge capture and supply of digital information in the future is having effective and cost efficient software that manages this information. s. 9(2)(j) OIA

Out of scope

s.9(2)(g) OIA

		Contact Phone No.
Briefing prepared by:	s.9(2)(a) OIA Manager Response Capability, Response & Operations	s.9(2)(a) OIA
Briefing reviewed by:	Jeremy Wood, Director, Policy & Partnerships	s.9(2)(a) OIA

14 December 2018

Assistant Commissioner: Response and Operations

Taser 7 and Associated Technology Briefing

Current Situation

1. A briefing (Appendix 1) regarding the new opportunities with Taser 7 was provided on 22 November 2018.
2. NZ Police has previously considered body worn cameras and found:
 - a. Body Worn Cameras (BWC) are an effective tool for police, providing important benefits that help prevent and resolve crime and make our staff and the public safer;
 - b. BWC do have issues and risks, which may be mitigated with careful consideration;
 - c. BWC are not beneficial unless they are complemented with an efficient and effective information management system, s. 9(2)(j) OIA [REDACTED];
 - d. New Zealand Police has been capturing footage of operating for over a decade (Tasercam), but do not use BWC currently. We do s. 9(2)(j) OIA [REDACTED] manage an increasingly large amount of digital information;
 - e. New Zealand Police are well placed to introduce BWC as we already have a tried, proven and functional digital information system to support BWC s. 9(2)(j) OIA [REDACTED];
 - f. Capturing digital footage, without information management support, provides little benefit. The benefit is when the digital information has meaning or relevance. s. 9(2)(j) OIA [REDACTED]
[REDACTED] Having BWC without information management support would produce more risk than benefit;
 - g. s. 9(2)(g) OIA [REDACTED]

Opportunities for Proof of Concept Testing

3. Response and Operations held an initial stakeholders meeting to determine what the various work groups in Police seek to ascertain by using camera technology. A proof of concept for the camera technology should demonstrate to Police if and how cameras may be best used to support Our Business, by providing enhanced health, safety and service delivery.
4. Road Policing, Criminal Investigations and Legal Section were consulted. Prevention staff were unable to attend.
5. Further consultation is anticipated including: District, ICT; Mobility; Human Resources; Service Organisations; Legal Services; Criminal Justice Support Unit; Prosecutions; Strategy Group; Corporate Instruments; Prevention, and Policy and Partnerships.
6. To keep the scope "tight" it is suggested that imagery is only captured:
 - a. when attending high priority incidents;
 - b. for safety and use-of-force recording¹; and
 - c. for family harm incident evidential videos.
7. Axon camera technology provides:
 - a. Camera Kit (Axon Body 2) - HD quality video, full-shift battery (12+ hours), wireless activation, and much more in a compact form factor; and
 - b. Axon Dock - for up to 6 cameras. Automatically offloads data and charges cameras (Does not require an associated computer);
 - c. Axon Fleet 2 (for vehicles)². s.9(2)(g) OIA [REDACTED]
 - d. Basic Licence - s.9(2)(b) OIA [REDACTED]
or
 - e. Pro Licence - s.9(2)(b) OIA [REDACTED]
8. s.9(2)(b) OIA , s. 9(2)(j) OIA [REDACTED]
9. It is recommended that a control group with Taser X2's be used to monitor differences with a variety of groups supplied with Taser 7s and the member's body-worn camera. The benefit of doing this with the Taser 7 is that the newer technology will reduce the administration time and pre-op checks for staff who will have additional checks and information management to complete with their cameras. It also provides a proof of concept for Taser technology to replace the current fleet that becomes obsolete in 3-5 years.
10. The probable groups are:
 - a. s.9(2)(g) OIA [REDACTED]

¹ When it is anticipated that a use of force report may be required.

- b. s.9(2)(g) OIA
[REDACTED]
[REDACTED]).

11. Each of these groups would have sub groups that:
 - a. don't record their activities by mobility cameras;
 - b. record their activities when attending high priority incidents, for safety and use-of-force recording; and
 - c. record their activities when attending high priority incidents, for safety and use-of-force recording, and for family harm incident evidential videos;
 - d. We would trial Taser's "Signal" (Bluetooth) technology for automatic activation when a firearm or Taser is drawn from their holster, or when a light bar is activated for Road Policing.
 - e. It will have to be determined if there are legal constraints preventing any of the intended uses.
12. It is thought that the benefits demonstrated by the Proof of Concept (PoC) will be that:
 - a. Suspect/witness behaviour will improve because they realise their actions are being recorded. This should result in less confrontational behaviour and fewer and less serious assaults on Police;
 - b. Recording of events will improve as the imagery will demonstrate what was:
 - i. observed by attending Police; and
 - ii. stated by suspects and witnesses. This should result in more accurate and efficient securing of evidence. Police will need to ensure that evidential sufficiency is correctly captured;
 - c. Officer behaviour should improve (compliance with policy/legislation) resulting in more moderate use of tactical options including fewer presentations of firearms. It is anticipated there will be fewer IPCA notifications, fewer complaints against Police and fewer not guilty pleas;
 - d. Police will need to ensure that the capture of imagery does not become overly burdensome. This will require consideration of:
 - i. the ability to store, search for, and retrieve, information;
 - ii. OIA requests;
 - iii. Public Records requirements;
 - iv. privacy issues; and
 - v. transcription/pixilation requests.
 - e. To inform the proof of concept (if approved) it is intended to use the Evidence Based Policing Centre to complete an international literature review to determine what assumptions should be made, and provide advice (along with the Tactical Options Research team) to ensure the survey that accompanies the PoC asks the right questions for NZ Police.
 - f. The Tactical Options Research team has provided data to demonstrate where the greatest benefit for Police is likely to be realised by a PoC. That data shows that the highest proportional use (per 10,000 Recorded

Criminal Offence Statistics (RCOS)) of all districts (with the exception of assaults on Police) is:

- i. 332 Tactical Options Reports (TOR) (with no Taser statistics included⁴);
 - ii. 135 assaults on Police (second highest - Tasman 155);
 - iii. 40 notifications to IPCA (with no Taser statistics included); and
 - iv. 22 firearms used as a tactic.
- g. Wellington is that district. This should ensure the frequency of use and severity of consequences are most likely highest and consequentially will demonstrate the greatest change in:
- i. benefits (health, safety and operational response); and
 - ii. challenges (information management impacting on service delivery after response).
- h. There may also be the opportunity to live stream video to the DCC and Communications Centre.

Recommendations

1. That the Police Executive consider the trial of camera technology for body-worn, and in-car, cameras s. 9(2)(j) OIA, with deployment of Taser 7. Yes/No
2. That the Police Executive direct that a detailed Proof of Concept for use of the Taser 7 with camera technology be designed to commence on 1 July 2019. Yes/No
3. Direct that a business case determine the full cost of the scoping project. s.9(2)(b) OIA , s. 9(2)(j) OIA Yes/No
4. That the Police Executive direct the proof of concept determine the benefits and challenges that may be realised by using body-worn and in-car cameras, for use where current legislation (Family harm incidents) or safety and use of force monitoring may be required. Yes/No
5. That the Police Executive direct the proof of concept be used in the district where the benefits and challenges are most likely to be demonstrated (the evidence is that this is Wellington District). Yes/No

□

Briefing prepared by:	Contact details
s.9(2)(a) OIA Operations Manager: Capability	s.9(2)(a) OIA
Consulted:	
s.9(2)(a) OIA , Coordinator Tactical Equipment Capability	s.9(2)(a) OIA 02
Briefing reviewed by:	
s.9(2)(a) OIA Manager Capability	s.9(2)(a) OIA

⁴ demonstrate little difference. Please note that with Taser 7 multiple cameras in the vicinity may be activated.

**POLICE EXECUTIVE MEETING (PEM)
COVER SHEET**

REFERENCE	PEM/13/78
TOPIC	Taser Camera Systems
SPONSOR	Assistant Commissioner Operations, Mike Rusbatch
PRESENTER	National Manager Operations: Superintendent Barry Taylor
MEETING DATE	Monday 23 September 2013

PAPER PREVIOUSLY CONSIDERED BY: (subcommittees / other committees)

- | | |
|---|--|
| <input type="checkbox"/> Police Executive Committee (PEC) | <input type="checkbox"/> Assurance Committee |
| <input type="checkbox"/> Police Executive Meeting (PEM) | <input checked="" type="checkbox"/> Other: OAC |
| <input type="checkbox"/> PEM Finance Committee | |
| <input type="checkbox"/> National Tenders Board | |

CONSULTATION:

The attached paper may have implications for the following work groups/service centres/districts whose views have been sought and are accurately reflected in this paper. Note: consultation with National Managers is compulsory unless directed by your executive sponsor. If the paper sponsor deems this consultation unnecessary, a full explanation needs to be provided in this section.

The names of those people consulted and their feedback must be recorded in the consultation table which is attached as an appendix to this template.

<input checked="" type="checkbox"/> NM: Policy <input checked="" type="checkbox"/> NM: Finance <input checked="" type="checkbox"/> NM: Legal <input checked="" type="checkbox"/> NM: Operations <input checked="" type="checkbox"/> NM: Prosecutions <input checked="" type="checkbox"/> NM: Training & Development <input checked="" type="checkbox"/> NM: Criminal Investigations <input checked="" type="checkbox"/> NM: International Services Group <input checked="" type="checkbox"/> NM: Planning and Performance <input checked="" type="checkbox"/> NM: Assurance <input checked="" type="checkbox"/> NM: Communications Centres <input checked="" type="checkbox"/> NM: Road Policing <input checked="" type="checkbox"/> NM: Professional Standards <input checked="" type="checkbox"/> NM: Financial Crime Group <input checked="" type="checkbox"/> NM: Prevention <input checked="" type="checkbox"/> NM: Mobility <input checked="" type="checkbox"/> Chief Technical Officer <input checked="" type="checkbox"/> National Property Manager <input checked="" type="checkbox"/> Manager: Strategic Communications <input type="checkbox"/> HR Manager: National Services & PNHQ <input type="checkbox"/> Director Organisational & Employee Development <input checked="" type="checkbox"/> Deputy Director: Intelligence <input checked="" type="checkbox"/> Deputy Director: OFCANZ <input checked="" type="checkbox"/> EMS Manager	<input checked="" type="checkbox"/> Commissioner <input checked="" type="checkbox"/> Deputy Commissioner: Operations <input checked="" type="checkbox"/> Deputy Commissioner: Resource Mgmt <input checked="" type="checkbox"/> GM: Finance <input checked="" type="checkbox"/> GM: Strategy, Policy & Performance <input checked="" type="checkbox"/> GM: MPES <input checked="" type="checkbox"/> GM: HR <input checked="" type="checkbox"/> GM: Public Affairs <input checked="" type="checkbox"/> AC: Operations <input checked="" type="checkbox"/> AC: Investigations & International <input checked="" type="checkbox"/> AC: Upper North <input checked="" type="checkbox"/> AC: Lower North & South <input checked="" type="checkbox"/> AC: Road Policing <input checked="" type="checkbox"/> Director: Intelligence <input checked="" type="checkbox"/> Director: Change <input checked="" type="checkbox"/> Chief Information Officer <input checked="" type="checkbox"/> District staff: District Commanders Auckland, Waitemata & Counties..... <input checked="" type="checkbox"/> External: Tactical Options Community Reference Group..... <input type="checkbox"/> Other (specify).....
--	---

TRACKING: (for EMS use only)



POLICE EXECUTIVE MEETING

REFERENCE : PEM/13/78
TOPIC : Taser Camera Systems
SPONSOR : Assistant Commissioner Operations, Mike Rusbatch
PRESENTER : National Manager Operations: Superintendent Barry Taylor

23 September 2013

Proposal

1. The purpose of this paper is:

- advise the Police executive of the commencement of the Taser replacement programme, beginning in pan Auckland districts in November 2013;
- seek approval for a district level trial of Taser body worn cameras, as an alternative to the Tasercam, in the Auckland district;

Background

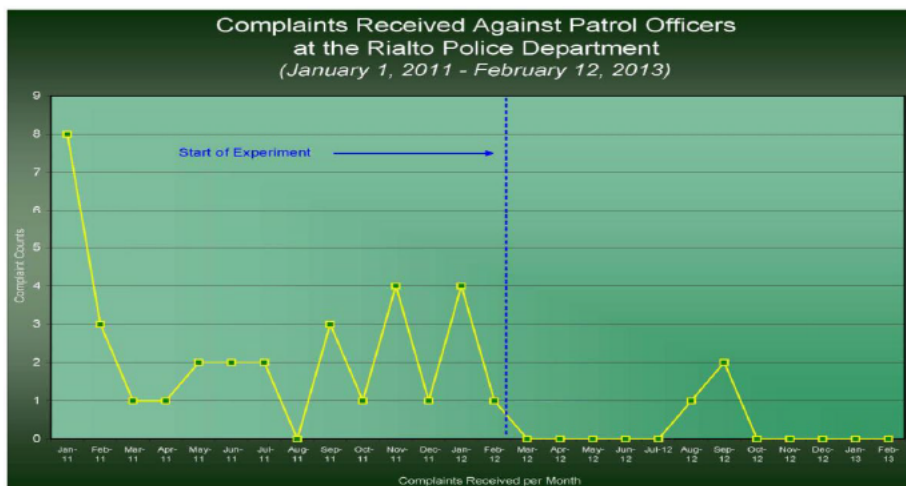
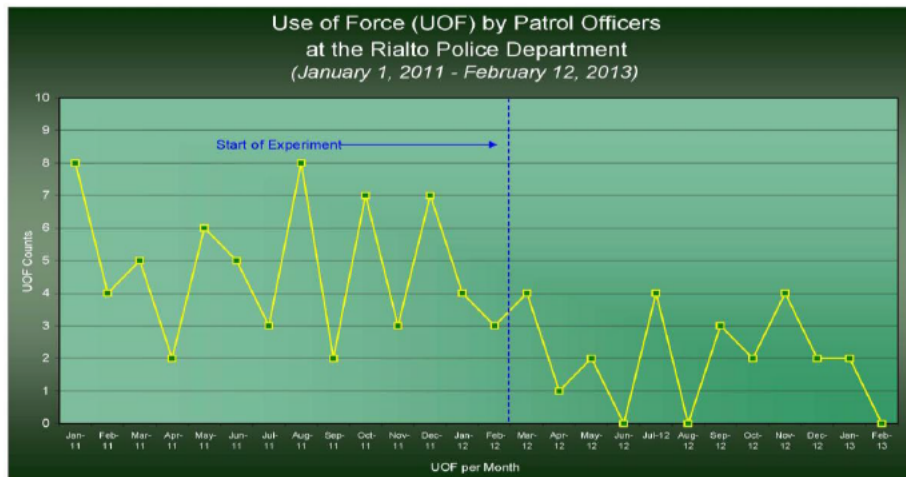
2. The Taser X26, as currently deployed in New Zealand, was developed in 2003 and when introduced in New Zealand in early 2010 it included Tasercam, a rechargeable power source that incorporated integral audio and video record capability with the battery system that operated the Taser.
3. In May 2013, as part of a scheduled replacement programme for Taser, the New Zealand Police utilised annual Taser allocated funding from the 2012/2013 financial year to purchase 238 X2 Taser. The X2 Taser, as a more technologically advanced, multiple shot device, was the preferred replacement option. At the time of the X2 purchase, decisions on the power source and the type and nature of the camera to accompany the Taser were deferred.
4. Allocated central government Taser funding for the 2013/2014 year is to be utilised to purchase the required power source, camera, associated support equipment and training requirements to enable the replacement programme which is scheduled to commence in November 2013 in the pan Auckland (Waitemata, Auckland, Counties Manukau districts) area.

The case for cameras

5. Taser continues to be internationally controversial technology and the New Zealand operating model, incorporating a camera system, providing assurance and accountability, is recognised as, and representative of, Australasian best practice.
6. The use of Tasercam in New Zealand police has enhanced operating practice, resolved complaints, assisted in enquiries (e.g. IPCA investigations, homicides etc) and has been presented several times as evidence. Tasercam, unlike body worn cameras, captures the point in an incident when force is used, it often does not always capture the wider context of an incident, where the decision to use force is formed. This can result in footage, which on face value, can appear to be unjustified force requiring extensive explanation.
7. With over 26 police forces in the United Kingdom alone deploying body worn cameras, use of camera technology in the general policing environment is widely positively reported on in

overseas jurisdictions with tangible benefits being cited as reduced complaints, reduced use of force, and reduced court time in terms of not guilty hearings. It is a tool that moderates both offender and officer behaviour positively and in that sense has a preventative effect.

8. The most recent published study from North America (Cambridge University) involved Taser Axon Flex body worn officer cameras in the Rialto police. Over a 12 month period the police department recorded a 59% reduction in the use of force and a corresponding 87.5% reduction in complaints against police.



9. s.9(2)(g) OIA [REDACTED] the type of camera system moving forward and the potential for future expansion of its use within a general policing context are critical factors that need to be addressed.
10. Available camera systems present issues in terms of proprietary software to synchronise, upload and securely store digital data from the cameras. Currently, the New Zealand Police operate Evidence.Sync and Evidence.Com, Taser systems which support all Taser propriety hardware.

Options

11. A (Tasercam)



HD Tasercam is the latest integral system developed by Taser, unlike its predecessor it has an exchangeable rechargeable battery. The camera is activated when the safety on the Taser is disengaged, most often when the officer has already made a decision to show or use force resulting in footage that often lacks the context of what the officer encountered.

The most cost effective of the options currently available due to the efficiencies of utilising a single rechargeable power source for both the Taser and the camera.

12. B(Axon Body)



The latest stand alone system developed by Taser. Positioned on the front of the current NZ Police body armour a high definition colour camera, incorporates 12 hour standby mode with 30 seconds buffering allowing officers to back capture events. Officer activated, 130° field of view, greater context is able to be captured. Due to carriage position view can at times be obstructed by officer's hands.

The camera is rechargeable, being a sealed unit the batteries have an estimated two year service life at the end of which the entire unit requires replacement. Separating the power source from the Taser has the advantage that serviceable Tasers will not be withdrawn for camera faults, however with that comes the additional annual cost of separate external power sources for the Taser.

13. C(Axon Flex)



The flex body worn camera has a separate camera, linked to the controller by means of hard wiring. The desirable camera position is on the head where point of view filming provides the officers true perspective of an incident. Officer activated, HD colour camera, 12 hour standby mode with 30 seconds buffering allows officers to back capture events.

The controller is a sealed unit which incorporates the power source and has a two year service life, at the end of which it requires replacement. The Axon Flex unit has been subject to a limited trial in the Wellington District alongside Tasercam at Taser incidents. The captured footage was better contextually than Tasercam footage however, staff on the whole didn't favour the available head mounting systems or the hard wiring between the camera and controller, which had to be assembled and disassembled from the body armour at the start and completion of each shift. Separating the power source from the Taser has the advantage that serviceable Tasers will not be withdrawn for camera faults, however with that comes the additional annual cost of separate external power sources for the Taser.

14. D(Tasercam/Axon Body)

Option D is an option whereby an operational trial can occur that compares the Tasercam (option A) and the Taser body camera (option B). The trial will allow for comparison of the benefits and risks, operationally, functionally, commercially commensurate with public perception. This option will allow continued Taser operating, providing the opportunity to exercise due diligence in terms of a Taser camera system that is fit for purpose and value for money. It is proposed that the trial will inform and guide the ongoing national Taser replacement programme.

Risks/Opportunities

16. While each option has advantages and disadvantages (refer Annex 'A') the New Zealand police has a unique opportunity to, within the current operating budget and Taser programme to trial body worn cameras, as an alternative to Tasercam and have a clearer picture of the future benefits and risks that each Taser camera system has.
17. By staying within the Taser suite of products, this opportunity allows us to trial their latest technology alongside their existing technology without risk to current operating practices s. 9(2)(j)
18. The scope, size and length of the trial would be sufficient to inform the organisation as to whether or not the tangible benefits of body worn cameras reported overseas are realisable within the New Zealand environment. A limited trial of the camera technology in Wellington was well received, the concept and technology being strongly supported by the participating staff.
19. In terms of public reaction to the increased use of cameras by police, the Tactical Options Community Reference Group has expressed that the debate surrounds public assurance, in terms of process [security] uploading, storing and management of information. Limited access rights, audit, disclosure controls need to be applied to prevent privacy breaches. Current Evidence.com software as deployed within the NZ Police Information technology systems is currently satisfying and will be able to continue to satisfy these needs.

Financial Implications

20. s.9(2)(f) OIA
21. s.9(2)(f) OIA
22. The financial implications of the options considered (listed above in para 11-14), including the preferred option, option D, are attached hereto as Annex 'A'.

IT Implications

23. Tasercam footage has been securely uploaded and stored within Evidence.com for the last 6 years. Evidence.com is Taser's secure evidence syncing, uploading and storing software that manages all Tasercam footage and meta data.
24. s. 9(2)(j) OIA, s.9(2)(g) OIA

s. 9(2)(j) OIA, s.9(2)(g) OIA

25. Evidence.com is currently undergoing an upgrade s.9(2)(b) OIA

Māori, Pacific and Ethnic Peoples

26. There are no implications for Maori, Pacific and Ethnic peoples.

Relationship to Key Outcome Areas

27. Taser can be directly linked with the NZ police strategic vision, mission and objectives: It provides safer communities by preventing the continuance of violent crime, enhancing public and police safety and ultimately ensuring that New Zealanders can be safe and feel safe.
28. Tasercams were initially introduced to provide the public with confidence and assurance that Police could utilise the Taser responsibly. Since its introduction the Taser cameras have also provided valuable insight into the behaviour of the offender, victim and officer at an assaultive and violent incident. They provide a mechanism whereby continuance improvement can and does occur in our training, and operating as a result.
29. Body worn cameras, the next evolution of Tasercam, provide further crime prevention benefits:
- international studies reveal body worn camera systems have a substantial impact in terms of moderating offender behaviour (resulting in fewer use of force by police) which in turn reduces victimisation, enhances public and police safety and reduces crime (be safe) and enhances the feeling of safety (feel safe);
 - those same studies reveal less complaints against police (officer moderation that enhances public trust and confidence) and improved number of guilty pleas and early guilty pleas (reducing demand on the Justice sector);
 - in terms of 'continual improvement' and public reassurance, the body worn camera system provides visual and audio context to an incident that Tasercam does not. It records the interaction between police, offender and victim prior to the use of, and after the use of, a Taser. It will capture critical and compelling evidence that provides both assurance and evidence;
 - given the body worn camera system's crime prevention capabilities (through offender behaviour moderation) it can be potentially utilised in all public interactions into the future which could have a significant impact in terms of reductions in the number of police complaints

Legislative Implications

30. New Zealand Police have been recording police, offender, victim interactions for over 6 years, using Tasercam, without issue. We have been recording and capturing still images of the public, offenders and victims for many years, in a public place. s.9(2)(g) OIA
31. The use of a body worn camera system in a private place is governed by the Search and Surveillance Act 2012. Body worn cameras, as well as Tasercams, are defined as visual surveillance devices. Their use does not require a surveillance device warrant provided they are on a private place lawfully and they [police] only record what the enforcement officer could see or hear normally without the use of such a visual surveillance device.

32. This makes the selection of the camera system, whether on the body or on the device critical, to ensure it captures only what would normally have been seen or heard, without enhancement, by the attending officer(s). s.9(2)(g) OIA, s.9(2)(j) OIA
- Taser body worn cameras and Tasercam are configured in such a way that they meet the requirements of the Search and Surveillance Act 2012, in that, as a visual surveillance device, they do not enhance footage beyond that of the normal vision and hearing of the attending officer.

Training and Implementation Implications

33. Taser operator trained staff are already familiar with the Taser and will undergo transition training to upskill them in terms of the enhanced functionality of both the Taser X2 and the Taser body worn camera system.
34. TSC have planned for and allowed transition training time for the Taser X2 and Taser camera system training nationwide, commencing in pan Auckland in November 2013. The transition training course for the Taser X2 and Taser camera system (both Tasercam and body worn camera system) has already being developed and is approved by the TSC training approvals committee.
35. Some training modification maybe required pending the outcome of this paper and any related policy implications.

Other Agencies

36. The Ministry of Primary Industries (old MAF) is the only known agency in New Zealand currently utilising body worn cameras.
37. The technology has improved and the cost has dropped significantly to the point where they can be commonly purchased. The private security industry is rapidly realising the benefits of body worn camera systems and many bouncers, noise abatement officers and security guards now have systems available to them for use.

Public relations

38. Communication will be necessary to advise staff of any implementation of next generation Taser X2's and body worn cameras. A communication plan, specific to pan Auckland in this instance, will be developed and implemented over the coming months in conjunction with the training and rollout. The communication plan will carefully highlight the trial of body worn cameras as police seek to understand the best Taser camera system to implement as part of the national Taser replacement programme.
39. Communications have already occurred in terms of the Taser X2 as the endorsed replacement for the Taser X26. National Manager Operations, in conjunction with Public Affairs, has already conducted several TV interviews regarding the Taser X2 as the replacement for the Taser X26.
40. Those few staff that have already trialled a body worn camera system endorse the use of body worn cameras 100%. Internal communications emphasising the benefits of body worn cameras (reduced complaints against police, reduced levels of force etc.) will be critical to embedding their employment. The Taser X2 transition training will be an ideal opportunity to communicate with a captured audience of staff and the transition training will cover off the reasons for the trial of body worn cameras, their benefits, how they work and the policy regarding their use.

Consultation Refer to feedback table attached as an appendix to this paper.

42. External consultation with the Tactical Options Community Reference group regarding the Taser X2 and Taser body camera system has occurred. They are not in a position to fully

endorse these options, as they understand police's choice and reasons to introduce Tasers, they are indifferent about Tasers in general. But neither did they raise any objections to these options. They understood the benefits that these options could provide.

43. One area they particularly emphasised was that having no camera system with the Taser would be a backward step in terms of public assurance and confidence that police use the Taser responsibly. s.9(2)(g) OIA

44. s.9(2)(j) OIA

45. Feedback was received from a number of areas. A common theme related to the extended use of body worn cameras beyond the scope of this paper. The trial of body worn cameras will be able to better inform us regarding their risks and benefits should it ever be proposed that body worn cameras be extended beyond the use of Tasers.

46. s.9(2)(g) OIA

The Privacy Commissioner has previously considered footage obtained by the use of police Tasercams. Her concerns were to do with the way police managed that footage and released that footage, especially to media. Her view at the time was informed consent was required from the individuals on the footage before any disclosure took place - these rules are applied in the disclosure (through OIA requests) of Tasercam footage and would be applied for body worn camera footage.

Recommendations

That the Police Executive Meeting:

- (i) note that, with executive approval, Taser X2's were purchased in the 2012/2013 FY in preparation for the commencement of the Taser national replacement programme, commencing in pan Auckland in the 2013/2014 FY (November 2013).
- (ii) note that a future Taser camera system is yet to be determined and that, from available Taser camera systems, a district level trial of Taser body worn cameras (in Auckland district), alongside the current Taser camera system (HD Tasercam), and in conjunction with the pan Auckland Taser replacement programme, is recommended.
- (iii) note that the preferred Taser camera system will be determined by the trial. The ongoing national Taser replacement programme and the identified preferred Taser camera system will be the subject of a future PEM paper.
- (iv) s.9(2)(f) OIA
- (v) s.9(2)(f) OIA
- (vi) s.9(2)(f) OIA
- (vii) endorse the trial of the Taser Axon body worn camera in Auckland District (option D) to evaluate the benefits of the body worn camera and inform the organisation of the preferred camera system to be utilised within the ongoing National Taser replacement programme.

- (viii) direct the National Manager Operations to commence the Taser replacement programme, beginning in pan Auckland and including, within it, the trial of the Taser body worn camera in Auckland district.
- (ix) direct the National Manager Operations to report back to PEM the outcome of the body camera trial and, based on these outcomes, make recommendations for the executive to consider, alongside approval for the continued national replacement of Tasers, the preferred Taser camera system.

Mike Rusbatch
Assistance Commissioner Operations

Consultation for PEM Papers

Reference: PEM/13/78
Topic: Taser Camera Systems
Executive Sponsor: AC Mike Rusbatch
Date paper sent for consultation: 10th September 2013

Please note consultation with National Managers is mandatory for every PEM paper. Any exceptions to this must be by the agreement of the Executive Sponsor of the paper. Please use the 'National Manager' group email address for consultation purposes (Executive & Ministerial Services team will keep the group email list updated).

Please clearly state if no response is received.

[illegible]

[illegible]

ANNEX 'A'

[illegible]

Option B Fully Funded Greater Auckland - Axon Body TSC Contribute Training

[illegible]

The image contains two anatomical diagrams of a human torso, showing internal organs. The left diagram is a frontal view, and the right diagram is a lateral view. Both diagrams include labels for the trachea, heart, lungs, stomach, and intestines. The diagrams are rendered in a simple, stylized manner with black outlines and white fill.

Option C Fully Funded Greater Auckland - Axon Flex TSC Contribute Training

[illegible]

s.9(2)(b) OIA , s.9(2)(j) OIA

[illegible]

[illegible]

Initial Concept Paper

<p>ID</p> <p>CP00034</p>	<p>On Body Camera Proof of Concept</p> <p>19th December 2014</p>
--------------------------	---

Police Operational Area

<p>Operations</p>

Police Operational Contact

Police Exec Member

<p>s.9(2)(a) OIA</p>	<p>Dept Commissioner Mike Clement</p>
----------------------	---------------------------------------

Background

New Zealand Police (NZP) undertook an unofficial trial of a very small number of differently configured on-body cameras (OBC's) for the purpose of understanding the best possible setup operationally.

In 2013, Response & Operations prepared a Business Case for consideration that focussed on trialling an OBC system to replace the failing (due to age) Tascam.

The case was submitted but declined for approval as, at the time, the NZP Executive felt the timing was not right for such a trial, the technology benefits were not well understood or advanced in policing and there was uncertainty in terms of public perception, privacy and legal justification surrounding OBC's.

With the advent of improved technology capability, successful evidence based international trials, legal opinions and the Policing Excellence the Future Programme, the option of OBCs should be considered again. The introduction of OBC's will drive initiatives to reduce family violence (Safer Families), improve evidential sufficiency, reduce complaints against police and improve our ability to capture valuable "evidence" in the field thereby supporting Evidence Based Policing.

Part of the current Taser solution includes the collecting, managing and presentation of the "digital evidence" via Evidence.com which is the evidential and digital management system that is available enterprise wide to every member of Police.

s.9(2)(g) OIA

Police at present are only using a very small part of the evidence.com capability (Tascam footage is the only digital evidence on it) s.9(2)(g) OIA

Furthermore, the IPCA has recommended that in particular, for family violence situations, video recording of victim complaints (at the scene) will likely provide better evidence, increase the chances of a successful prosecution, decrease the time spent by Police in Court and provide a better overall experience for victims.

Finally, a significant international study undertaken by Cambridge University (Rialto) showed that by deploying body cameras and recording events leading up to and during an “incident”, reduced the number of “use of force” complaints and increased the “conviction rates” of domestic violence offenders.

Description of Problem

Having an “authoritative source” for digital evidence is a key theme of Police’s ISSR and will ensure that the evidentiary value of that evidence is preserved and not compromised throughout its lifecycle.

s.6(c) OIA

Additionally, the ongoing cost of replacing and maintaining Tascam, as the Taser fleet ages, is becoming prohibitive (due to its impact on operational Tasers when the battery life corrupts footage).

Therefore, separating the camera from the power source is regarded as a solution to this problem.

Taser units that are currently deployed incorporate a built-in camera which also incorporates the Taser power source.

Lessons learned in the Taser programme over time, reveal that as Tasers age, the battery condition deteriorates which can corrupt the camera footage and affect its operational & evidential credibility.

A simple solution to this costly problem is to remove the power source from the camera - OBC's would achieve this.

There are also inefficiencies around docking and categorising of data and it appears OBC's will help improve this.

The current Tascam setup also reduces the ability to capture footage leading up to an incident as the camera is only activated once the Taser is removed from its holster.

High Level Requirements

With the introduction of the X2 Tasers, the ability to “decouple” the Taser from the camera is now possible which reduces the risk of information being lost or corrupted due to degraded batteries.

A more cost effective means for upgrading our Taser fleet is necessary and with an OBC solution, replacement will be less costly than the traditional Taser/Camera solution.

As we replace the fleet of X26's with the X2's, the overall cost of upgrading the Taser units will reduce, therefore reducing our total cost of ownership of the devices.

A Proof of Concept (PoC) is being recommended to prove the real value to Police of incorporating OBC's.

It is being suggested a PoC be undertaken in the Bay of Plenty District with operators in response vehicles. This will equate to approximately 90 Taser/OBC units and will be achieved by upgrading the current X26 Tasers with the X2 plus an OBC.

An alternative option may be, for a two man "response vehicle", one responder would be the designated "Taser Operator".

Upon arriving at an incident, the camera would start to record, capturing an area of 120 degrees in front of the officer as well as recording audio in and around the incident (providing a more concise record of the incident and the discussions that occurred).

The OBC for the PoC would be used for family violence incidents, both in public and in private and at incidents where a Taser would normally be drawn from a holster.

s.9(2)(b) OIA

It is anticipated that upon returning to the station, the data would then be uploaded into evidence.com, categorised and then made accessible (longer term, potentially through a mobility app onto Police iPhones and or potentially "linked" to the CARD event).

Additionally, there is a need as part of the PoC to provide some quantitative measures for Police to measure the effectiveness of deploying such devices. This will require the involvement of the Performance Group to provide statistics and measures of historical offences and prosecutions (relating to domestic violence) before and after deployment in the BoP District.

Funding

- PoC devices will be provided from the 2014/15 Operations Taser replacement budget.

- s.9(2)(b) OIA

- Response & Operations will fund the entire PoC (including ICT costs) from their 2014/15 Taser Replacement Programme.

Risks

- Unavailability of evidence.com;
- Sufficient storage and processing capability;
- Availability of resources: both ICT and business;
- Availability of Police front-line personnel to undertake the PoC;
- Insufficient evaluation of the trial leading to poor future outcomes.

Benefits

Recently the UK College of Policing and Essex Police completed a study relating to the use of OBC's during family violence incidents. The results showed an increase in the number of successful prosecutions for family violence offences (when the OBC was involved) but without an increase in the overall number of reported family violence incidents.

The increase in successful prosecutions was greatest at the lower level of family violence offending (which is the most voluminous part of offending). Additionally, officers who used the OBC's reported greater confidence in the ability to capture evidence (especially contested evidence between victims and offenders, such as allegations and admissions) and greater mindfulness of their own behaviour during public/victim/offender interactions.

Indicators of primary and secondary findings and benefits from international experiences of such OBC trials include:

- increase in the number of successful family violence prosecutions and convictions without an increase in the number of reported offences (primary);
- efficiency improvements during the response, investigation and prosecution of family violence - example of a key indicator are less abstractions from front line for family violence court appearances (primary);
- improved family violence risk assessments from readily accessible and timely digital information (primary);
- improved quality and consistency of sufficient evidence to support the completion of a family violence complaint (contemporaneous admissions and allegations which are often rescinded before court) (primary);
- reduction in complaints against police (secondary);
- reduction in the use of force by police (secondary);
- improvements in officer behaviour when interacting with victims, witnesses, offenders and other subjects (secondary);
- improvements in lessons learned, training and debriefing for officers when attending family violence incidents (secondary);
- accurate and quality notes and correspondence - the officers account of events is fully

supported by the single point of truth,;

- video - fully reviewable digital information that is retrievable in a timely manner that officers can review from mobility devices (secondary);
- integrity of digital files sustain the public's trust and confidence in the legitimacy of the criminal justice system;

Other benefits include:

- reduction in crime (focusing on family violence in the first instance);
- better evidence;
- increased prosecution rates;
- decreased time spent by Police, prosecutors and defence lawyers in Court;
- reduced "not guilty" pleas;
- a better overall experience for the victims through quicker timeframes for outcomes of cases and not requiring victims to attend court to give evidence;
- A mechanism for Police to potentially implement a consistent process nationally around preservation of digital evidence.

s.9(2)(g) OIA

Stakeholders & Governance

- Business Sponsor – TBC
- Prevention - NM Prevention as business owner for family violence;
- Response & Operations - NM Response & Operations as owner of capability (lead as owner for the trial);
- Crime - NM Investigations as owner of evidence, interviewing;
- ICT - as owner of the technology.

Core 4

- s.9(2)(a) - BPM
- TBC - Technical Owner
- TBC - Support Owner
- s.9(2)(a) - Business Owner



Police filming and audio recording of operations and events

Executive summary

This chapter outlines:

- Police policies relating to covert and open and observable video and audio recording by Police of Police operations and events
- approval requirements before operations and events may be recorded, including the need for approved equipment to be used
- the circumstances in which privately owned mobile phone recording applications and cameras may be used for Police purposes
- the circumstances in which Police-issued smartphones or tablets may be used to record photographic and video images
- requirements for ensuring any images taken will be accepted by the court as reliable evidence.

The key, critical points for staff to note are:

- Recording equipment must be Police-issued and approved.
- Approval is required for wearing covert or overt body worn cameras or recording devices.
- Fitting of any recording devices to Police vehicles requires approval of National Manager: Response and Operations and the Manager: Fleet Management.
- Your first option for collecting photographic or video evidence should be a Police photographer; however, if urgent, and a photographer is not available, then a smartphone or tablet may be used.
- Tasercam should not be used for the sole purpose of obtaining video and audio evidence.
- Where approval is given, it is permissible to record everything in a public place or on private property so long as the employee records only what they personally see and hear.
- Images or recordings taken on a police device must be downloaded or emailed to a police computer as soon as practicable.
- It is not an offence for members of the public to film or take photos of police employees carrying out their duties, and you have no powers to prevent this from happening.

This chapter should be read in conjunction with the Search and Surveillance Act 2012 and the 'Search' chapters of the Police Manual.

Recording equipment must be Police-issued and approved

Where visual or audio recording is approved for particular operations or events, (see 'Covert body worn cameras and video recording devices' and 'Open and observable use of cameras and recording devices' above), it should only be carried out using **Police issued and approved equipment** following standard purchasing practices.

All covert recording equipment must be supplied and approved by the Technical Support Unit (TSU). Except for cameras used by Police photographers and investigators for forensic or investigative purposes, any other equipment to be used to record Police operations and events must be approved by the National Manager: Response and Operations.

The requirements outlined in this chapter do not affect existing policies around the approval and use of cameras and recording equipment by specialist groups such as Police photographers, CIB (), STG (), or Road Policing for authorised purposes.

Benefits for Police of recording operations and events

Police routinely use cameras and video recordings in watchhouses, front counters, for investigations and in public places for road policing purposes. It is also normal practice for Police to record calls to its' Communications Centres.

Photographs, video and audio recordings of Police operations and events can also be valuable resources for briefings, orders groups, debriefings and subsequent enquiries. Video recordings are particularly useful for recording instructions or 'cease and desist' orders by operation commanders to counter subsequent complaints against Police employees.

Police photographers using still or video cameras may also be approved for deployment by the operation commander at demonstrations in some situations. (See the 'Operation commander' section in the 'Demonstrations' chapter for more information).

Media filming of Police operations and activities

See the 'Media filming of Police operations' Police Manual chapter for information about when media accompanying Police may film Police operations or policing activities.

Approval required for wearing body worn cameras or recording devices

You must have approval before:

- using any body worn camera or recording device (see the sections on covert and open and observable use below)
- fitting any video recording devices to Police vehicles.

Covert body worn cameras and other video recording devices

Covert body worn cameras, or other covert video recording devices or equipment can only be used to record policing activities with the prior approval of the Manager: Covert Operations Group at PNHQ.

Improper or unauthorised use of any covert recording equipment may compromise the effectiveness of other operations and the safety of Police involved in authorised covert policing activities. (See 'Covert backstopping' in the Police Manual for more information about using covert resources).

Specialist units such as the STG and AOS have authority to obtain and use covert equipment specific to their area of policing.

Open and observable use of body worn cameras and recording devices

Employees must not be overtly equipped with or use body worn cameras or other video recording devices (which may also include audio) to record policing activities without prior authorisation from the National Manager: Response and Operations.

Authorisation may only be given if the National Manager: Response and Operations is satisfied that the use of the camera or recording device is for a legitimate policing purpose and that there are strict controls and adequate safeguards in place to avoid breaching the Information Privacy Principles in the Privacy Act 1993, the New Zealand Bill of Rights Act 1990, Search and Surveillance Act 2012 and other relevant legislation.

It is expected that any authorisation given will be an individual exception and for a strictly limited period. This includes projects, trials and evaluations.

(See also 'Recording equipment must be Police-issued and approved' above).

Fitting devices to vehicles

Fitting of overt or covert video recording devices (which may also include audio) or other equipment to Police vehicles requires additional written approval (to that of the National Manager: Response and Operations) from the Manager: Fleet Management, PNHQ. See '[Police vehicle management](#)'.

Use of Police-issued smartphones and tablets

Police-approved smartphones and tablets are being increasingly issued and used for Police purposes as part of the Policing Excellence Mobility initiative. This chapter does not impose any additional approval requirements for their issue. However, the guidance in this chapter for the use of the phone's or tablet's recording applications applies.

While Smartphones and tablets have photographic, video and voice recording applications, your first option for the collection of photographic or video evidence should **always** be the standard Police procedures, i.e. **using the Police photographer or a Police-issued digital camera**. However, if there is an urgent and identifiable need to record the evidence and a photographer or Police-issued camera is not available, images may be recorded on the smartphone or tablet using the camera App within the secure environment.

A Police-issued smartphone may be used to record evidential interviews of family violence victims or complainants, but only as part of an authorised trial or proof of concept run by the National Prevention Centre.

Follow the procedures for '[Securing images taken on smartphones, tablets or personal cell phones](#)' if you take any images on a smartphone or tablet. Note however, that there may be limitations on using these images for evidential purposes later because of the difficulty of maintaining their original format during the process of downloading/ securing them.

Use of TASER cameras (Tasercam)

The Electronic Control Device approved for use by the New Zealand Police is the "TASER" X2 and the devices Tasercam records video and audio.

Under no circumstances should the TASER and Tasercam be employed or used in situations where the sole purpose of the deployment is the gathering of digital video and audio evidence. (See the '[TASER \(Conducted Electrical Weapons\)](#)' Police Manual chapter for more information).

Privately owned mobile telephones and cameras should not be used

Images should **not** be taken for Police purposes using non-Police issued equipment, unless there is an urgent and identifiable need to do so, e.g. where vital evidence would be lost or inclement weather would intervene before a Police owned camera or other recording device would be available.

Follow the procedures for 'Securing images taken on smartphones, tablets or personal cell phones' if any images are taken on privately owned devices.

Note however, that there may be limitations on using these images later for evidential purposes because of the difficulty of maintaining their original format during the process of downloading/ securing them.

What can be recorded or filmed?

Where approval is given, it is permissible to video record (may include audio) everything in a public place, or on private property when lawfully present, so long as the employee records only what they personally see and hear (i.e. you can not leave a camera recording while you move to another place on private premises out of sight or hearing of the camera). The video recording may be done overtly or covertly, and with or without the other party's permission.

Audio recording of interactions with the public

As a general principle, employees should not make audio / voice recordings of interactions with the public in a public place; however, one-off exceptional circumstances may exist to do so, but this should only occur if authorised by a District Commander, National Manager or by the National Manager: Response and Operations.

An example may be where it is necessary to visit a person who is a recidivist complainant about Police where there has previously been disagreement about what was said. In this circumstance the person should be advised that the conversation will be recorded to ensure that an accurate record is kept.

It is permissible to lawfully make audio recordings without warrant, so long as one party consents. (This is normal, permissible practice for the Police Communications Centres and the like).

Securing images taken on smartphones, tablets or personal cell phones

Images / recordings taken as evidence on Police smartphones, tablets or personal cell phones are subject to disclosure. It is therefore critical that all images / recordings taken are downloaded and secured as soon as possible in accordance with the Police Manual chapter 'Photography (Forensic imaging)'.

This ensures the images / recordings:

- are associated with the appropriate case file and will be disposed of when no longer required for legitimate policing purposes
- will be accepted by courts as reliable evidence and to minimise the risk of legal challenges around whether they could have been compromised.

Evidential images / recordings must not be retained on Police smartphones and tablets or personal cell phones or used for purposes other than for what they were intended.

Procedures for downloading and securing images

Step	Action
1	Record details (date, time and location) of the images / recordings in your notebook.

2	<p>Email or download all images / recordings to a Police computer as soon as possible after being taken. Ensure the images are saved according to your local standard operating procedures.</p> <p>Do not email or download images / recordings taken as evidence to a personal computer.</p> <p>The way in which the image should be downloaded will vary depending on the type of device. Follow the guidance on downloading and securing captured images to computer in the 'Digital imaging guidelines' section of the '<u>Photography (Forensic imaging)</u>' chapter where applicable. However, be aware that generally, downloading from smartphones, tablets or cell phones will alter the format and resolution of the image. These issues relating to evidential quality and reliability may limit the later use of the image for evidential purposes.</p> <p>If you are unsure of what to do in any case, seek advice immediately from your local Photography section.</p>
3	<p>Delete the images from the Police issued smartphone or tablet or privately-owned cell phone or recording device once they have been downloaded to a Police computer.</p>
4	<p>Any evidential images taken that are no longer required for legitimate policing purposes must be disposed of as soon as practicable. The standard retention and disposal periods apply in cases where the images are retained as part of Police files. See '<u>Retention and disposal of Police records</u>'.</p>

Public photographs of Police activities

Occasionally, members of the public film or take photographs of Police employees carrying out their duties. This is **not an offence** and **you have no power** to prevent the photographs being taken or to seize the camera or digital storage media.

Released under the Official Information Act 1982

Research on Body-Worn Cameras

Requested By: DCE Strategy Mark Evans

Prepared By: [REDACTED]

Reviewed and approved By: [REDACTED] Date: 18 April 2018

This Terms of Reference outlines the proposed research aim, objectives, approach, timeframe and resources, and expected output.

1. Aim

In April 2018, DCE Strategy Mark Evans tasked Research and Evaluation (R&E) at the Evidence-based Policing Centre to undertake a research project on body worn cameras (BWC).

2. Previous research

A recent rapid literature review conducted by Research and Evaluation in 2017 identified that a prospective meta-analysis of ten multi-site, multi-national randomised control trials covering 8 police forces in 6 jurisdictions reported two relevant findings. Ariel *et al.* (2016) found that despite the conflicting findings across sites, the combined results suggest that the use of BWC did not alter the rate of police use of force. Second, the combined results suggest that the use of BWC increased the risk of assaults on officers: the rate of assaults against police officers was 14% higher during the experimental condition, when compared with the control condition (25 vs 22 assaults per 1000 arrests). These findings contradicted the 'perceived wisdom' that BWC were an effective tool to reduce officer-related harm.

3. Research scope objectives

The research seeks to:

1. Identify the global use of BWC by policing agencies, including those agencies which have discontinued using BWC;
2. Collate and synthesise the empirical evidence around the impact of use of body worn cameras by police officers, e.g. officers' safety, officers' acceptability, and public perception;
3. Understand how BWC are used by other justice sector/regulatory agencies in New Zealand, and overseas;
4. Explore the evidence outlining the utility and functionality of BWCs in operational contexts;
5. Identify the legal, ethical, and cultural issues around the use of BWC in New Zealand.

4 Approach

The proposed approach will involve:

1. Collaboration and consultation with relevant groups

Given the nature and implications of this research to the operational environment, a collaborative approach will be taken. As a first step, Research and Evaluation will discuss the research objectives with the Response and Operations group to determine the formation of a consultation panel who will support, inform and review the research findings.

2. Review and synthesis of the literature and operational reports

The research will involve collating and synthesising published literature and unpublished reports. Literature and reports will be identified through a systematic search using academic databases and other electronic databases (e.g. google), news article searches, and making direct contact with organisations that may hold the relevant documentation. KAI will be tasked to source material.

Operational Reports by police agencies outside New Zealand will be sourced through formal channels of Police Liaison Officers in London and Washington, and informal channels through international evidence-based policing networks.

3. Potential review of legal and cultural considerations

Discussions will be held with other Police workgroups (identified through the consultation panel) to canvas the potential implications of introducing body-worn cameras at New Zealand Police. This may include a discussion of the legal and cultural considerations.

4. Consideration of alternative technologies

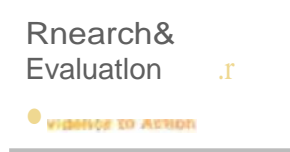
There may be relevant emerging technologies that could complement or replace BWC.

5. Timeframe and resourcing

Scoping	Apr 2018	0.25 Senior Researcher:	[REDACTED]
Consultation group membership and terms of reference determined	May 2018	0.25 Senior Researcher:	[REDACTED]
Literature and report searching	May-Jun 2018	0.20 Senior Researcher:	[REDACTED]
		0.25 Research Assistant:	[REDACTED]
Evaluation and synthesis	Jul-Aug 2018	0.25 Senior Researcher:	[REDACTED]
		0.10 Senior Researcher:	[REDACTED]
Report drafting	Sep – Nov 2018	0.50 Senior Researcher:	[REDACTED]
		0.10 Senior Researcher:	[REDACTED]
Interim report discussion DCE Strategy and Consultation Panel	Sep 2018		
Final report	Dec 2018	0.25 Senior Researcher:	[REDACTED]

6. Output

An interim report will be provided to the consultation panel for review and to the DCE Strategy by 30 September. The final research report will be provided to the Executive by 14 December 2018, which will outline findings relevant to the research objectives and provide recommendations on next steps.



Terms of Reference: Body-Worn Cameras Research

Requested by: DCE Strategy Mark Evans

Prepared by: [REDACTED]

Reviewed and approved by: [REDACTED]

Date: 18 April 2018

1. Aim

The aim of this research is to determine the evidence base on the rationale, use and effectiveness of body worn cameras, both nationally and internationally. The output of this research will be a report to Inform the New Zealand Police Executive's decision making on the potential use of body worn cameras (BWC).

2. Research objectives

The research seeks to:

1. Identify the global use of BWC by policing agencies, Including those agencies which have discontinued using BWC;
2. Collate and synthesise the empirical evidence around the impact of use of BWC by police officers, e.g. officers' safety, officers' acceptability, and public perception;
3. Understand how BWC are used by other justice sector/regulatory agencies in New Zealand and overseas;
4. Explore the evidence outlining the utility and functionality of BWCs in operational contexts;
5. Identify the legal, ethical, practical and cultural issues around the use of BWC in New Zealand.
6. Explore potential alternative technologies that may complement or substitute BWC.

3. Approach

The proposed approach will involve:

1. Collaboration and consultation with relevant groups

Given the nature and Implications of this research to the operational environment, a collaborative approach will be taken. As a first step, Research and Evaluation will discuss the research objectives with the Response and Operations group (and other relevant work groups -to be confirmed) to determine the membership of an advisory group. This group will support, inform and review the research findings.

The advisory group will also help identify relevant work already undertaken with New Zealand Police across the various groups on BWC (this will include work such as Research and Evaluation team's (2017) BWC rapid literature review). The work identified at this stage will form part of an initial stocktake and will be summarised in the final report.

2. Review and synthesis of the literature and operational reports

Both published literature and unpublished reports on rationale, use and BWC effectiveness will be collated and synthesised into the final report. Literature and reports will be Identified through a systematic search using academic and other electronic databases (e.g. google), news article searches, and through direct

EVIDENCE BASED — POLICING • CENTRE • • •

contact with organisations that may hold the relevant documentation. Police's Knowledge and Information services (KAI) will be tasked to source material.

Operational reports by police agencies outside New Zealand will be sourced through Police Liaison Officer channels in London and Washington, and international evidence-based policing network channels.

3. Potential review of legal, ethical, cultural and practical considerations In the New Zealand context

Depending upon the nature of the findings established In step 2 above, discussions may be held with other Police workgroups (identified through the advisory group) to canvas the potential implications of introducing BWC at New Zealand Police. This may Include a discussion of the legal, ethical, cultural and practical (e.g. storage) considerations. These considerations will be summarised In the final report.

4. Consideration of alternative technologies

There may be relevant emerging technologies that could complement or provide a substitute for BWC, for example victim video statement technology or Taser technology. The implications of using these alternative technologies to complement or substitute BWC will be discussed in terms of potential costs and benefits in the final report.

4. Timeframe and resourcing

Scoping	Apr 2018	Senior Researcher: [REDACTED]
Advisory group membership and terms of reference determined	May 2018	Senior Researcher: [REDACTED]
Stocktake of completed BWC New Zealand Police work drafted		
Literature and report collation	May-Jun 2018	Senior Researcher: [REDACTED] Research Assistant: [REDACTED]
Literature and report evaluation and synthesis	Jul-Aug 2018	Senior Researcher: [REDACTED] Senior Researcher: [REDACTED]
Potential review of ethical, legal, cultural and practical considerations		
Exploration of alternative technologies		
Report drafting	Sep – Nov 2018	Senior Researcher: [REDACTED] Senior Researcher: [REDACTED]
Advisory Group review and feedback on Interim report	Sep 2018	Senior Researcher: [REDACTED]
Interim report discussion with DCE Strategy		
Final report completed	Dec 2018	Senior Researcher: [REDACTED]

5. Output: Interim and Final Reports

An interim report will be provided to the advisory group for review and to the DCE Strategy by 30 September. The final research report, outlining research objective findings and recommendations on next steps, will be provided to the Executive by 14 December 2018.

New Zealand Police

Request for Information

Digital Information Management

TN/21/02

RFI released: 02 07 20

Deadline for Questions: 5pm 10 07 20

Deadline for Responses: 12.00 noon 21 07 20

New Zealand Police
Police National Headquarters
180 Molesworth Street, Thorndon
Wellington

Contents

This opportunity in a nutshell 3

SECTION 1: Key information..... 4

SECTION 2: Our Requirements 6

Appendix 1: RFI Questions & Response Form 10

This opportunity in a nutshell

What we need

Currently New Zealand Police (Police) receive and store a wide range of data from an equally wide range of sources including video interviews, CCTV footage, Taser videos, digital photos and forms, social media, Eagle helicopter footage and much more.

We need to understand what proven “off the shelf” technical solutions are available that will allow Police to efficiently and effectively manage, consume and analyse this diverse and ever increasing range of digital information.

What we don’t want

We do not want responses that are based on:

- Enterprise Content Management systems
- bespoke development
- consulting services or theoretical advice about abstract or speculative approaches
- solutions that only address a single type of digital information
- new and untested solutions.

What’s important to us

We are looking for proven and “off the shelf” digital information management solutions that will allow us to provide:

- More efficient and effective criminal investigations through the ability to provide the right information to the right people at the right time.
- Prevention of crime through improved and more targeted intelligence gathering and more “focused” preventative measures.
- The ability to better meet our legislative requirements around data retention and destruction.
- Improved analytics capability by having data in a single repository and able to be searched and analysed by multiple tools.
- Mitigation of financial risks due to exponential costs in storage
- For managing all types and sources of data whether it be evidential or non-evidential

Why should you respond?

Your response is a unique opportunity to directly educate and inform us about your digital information management solutions and how they can help make New Zealand the safest country.

A bit about us

The vision of Police is for New Zealand to be the safest country. Our mission is to prevent crime and harm through exceptional policing. With over 15,000 staff, we provide policing services 24 hours a day, every day. We operate by land, sea and air and manage over 860,000 emergency calls a year.

SECTION 1: Key information



1.1 Context

- a. This Request for Information (RFI) is an invitation to suitably qualified suppliers to submit a Response for the Digital Information Management process.
 - b. This RFI is intended to be the first step in a multi-step procurement process.
-



1.2 Our timeline

- a. Here is our timeline for this RFI.

Steps in RFI process:

Date:

Deadline for Questions from suppliers: 10 07 20

Deadline for the Buyer to answer suppliers' questions: 15 07 20

Deadline for Responses: 12.00pm 21 07 20

Responses reviewed and clarifications requested: 12 08 20

Notification to Respondents on conclusion of the RFI phase and any likely next steps: 11 09 20

- b. All dates and times are dates and times in New Zealand and are subject to change by Police at their sole discretion.
-



1.3 How to contact us

- a. All enquiries must be directed to our Point of Contact. We will manage all external communications through this Point of Contact.
 - b. No member of New Zealand Police is to be directly contacted or approached regarding this RFI and your Response.
 - c. **Our Point of Contact**
Title/role: Contracts Administrator, National Procurement Group
Email address: tenders.national@police.govt.nz
 - d. Suppliers may contact the Point of Contact for further clarification.
-



1.4 Developing and submitting your Response

- a. Take time to read and understand the RFI. In particular, develop a strong understanding of our Requirements detailed in [Section 2](#).
 - b. For helpful hints on tendering and access to a supplier resource centre go to: [www.procurement.govt.nz / for suppliers](http://www.procurement.govt.nz/for-suppliers).
 - c. If anything is unclear or you have a question, ask us to explain. Please do so before the Deadline for Questions. Email our [Point of Contact](#).
 - d. In submitting your Response you must use the Response Form provided in Appendix 1 of this document. This is a Microsoft Word document that you can download.
 - e. Your Response should be sequentially page numbered.
 - f. Check you have provided all information requested, and in the format and order asked for.
 - g. Having done the work don't be late – please ensure you get your Response to us before the Deadline for Responses!
-



1.5 Address for submitting your Response

Please submit your Response electronically.

a. Responses must be submitted by email to the following address:

Tenders.national@police.govt.nz

a. Responses sent by post or fax, or hard copy delivered to our office, will not be accepted.



1.6 Our RFI Terms and Conditions

a. Please be mindful of the following terms and conditions of this RFI:

- i. The issue of, and response to, this RFI is for information gathering purposes only and is not to be construed as representing or creating any binding obligation on Police to enter into any legal commitment whatsoever or as being any commitment by us to make any purchase of services.
 - ii. A response to this RFI will not confer any advantage on any organisation if any subsequent tender eventuates.
 - iii. You should identify any parts of your Response that are commercially sensitive. We will not, subject to our legal obligations (including under the Official Information Act 1982 and Privacy Act 1993) and our obligations to Parliament, provide commercially sensitive information to any third party except on an anonymised basis.
-

SECTION 2: Our Requirements

2.1 Purpose of this Request for Information

- 2.1.1 Police is looking to enhance the management of their digital information, and adopt tools to collect, manage, analyse, and integrate that data into Police internal systems and share with other Government Agencies.
- 2.1.2 This project is at the initial planning stage and the results of this RFI document will be used to:
- Gather information relating to the availability of digital information systems available in the world market
 - Understand the nature and composition of the supply market
 - Obtain indicative pricing for business case purposes
 - Refine business requirements
 - Aid in the drafting of an intended Request for Proposal (RFP). It is likely but not definite that an RFP will be drafted and released following this RFI process.
- 2.1.3 Please note that this RFI is for information purposes only – it will not be used to evaluate individual suppliers, will not be used to create a shortlist and will not result in a contract award. However, it is an excellent opportunity for the supply market to provide early input into this project.
- 2.1.4 Following receipt of the RFI responses Police may contact or meet with a selection of suppliers to gain further information; this will not confer any advantage on any supplier if a subsequent RFP eventuates.

2.2 Background

- 2.2.1 Police is the lead agency responsible for reducing crime and enhancing community safety in New Zealand. With nearly 15,000 staff, we provide policing services 24 hours a day and function from community-based police stations across the country.
- 2.2.2 Our functions are: Keep the peace, maintain public safety, law enforcement, crime prevention, community support and reassurance, national security, Policing activities outside of New Zealand and emergency management.
- 2.2.3 At present Police collects (or is provided) data from multiple sources. Examples are:
- Taser video;
 - Victim video iPhone statements;
 - CCTV (sent in by the public);
 - Digital photos;
 - Audio recordings;
 - Digital forms;
 - Facebook media; and
 - Eagle helicopter footage.
- 2.1.1 The data is in multiple formats and is currently stored in different systems both on premise and in the cloud.

- 2.1.2 The data can be used for evidential purposes (recorded from victim interviews for example) as well as non-evidential purposes (investigative or analytical). Non-evidential data is by far the largest and growing source of information being presented to Police.
- 2.1.3 Data integration across enterprise applications is point to point and in some cases labour intensive to link evidence with case files.
- 2.1.4 Data growth is 30% pa and cost is contained by moving archival data to lower tier disk specifications.

2.2 Requirements

- 2.2.1 This Request for Information relates to the possible technical solutions for Police to manage and analyse all digital information it creates or receives throughout its lifecycle and the consumption of that information by people and systems in the organisation as well as partners outside of the organisation.
- 2.2.2 Police intend to use the results of this RFI to help form their requirements, however some high level requirements have already been identified.

High Level Use Cases

- 2.2.3 These use cases have been provided to set the context within which we wish the solution to operate:
 - a) As a frontline officer I want to be able to upload video footage I have recorded or been provided so that it can be analysed, indexed and managed in a way that the appropriate people can access and use the information as required to complete their jobs.
 - b) As an intelligence user I want to be able to search all digital information looking for a particular item or reference (fuzzy or AI).
 - c) As a frontline officer I want to be able to upload information that I have recorded or gathered (video, audio or photographic, signed statements etc.) without needing to return to the station or download to an intermediate device.
 - d) As a frontline officer I want to be able to record an interview in an interview suite, upload the data and be confident that the chain of evidence is intact so that it can be presented and used in court.
 - e) As a prosecutor I want to be able to share access of an interview recording with a defence lawyer so that a fair trial can be held.
 - f) As an IT professional I would like to be able to easily associate data held in the digital management solution with data held in other Police systems so that an end user can have a complete picture of the information Police have on a specific case.
 - g) As a member of the public I would like to be able to upload video, voice recordings or photographs so that Police can use the information to help me.
 - h) As the CIO I want to be able to control storage expenditure so that public funds are used wisely.

High Level Requirements:

- 2.2.4 Any solution should be able to be broken down into three distinct delivery areas:
 - a) **CAPTURE** – The collection and ingestion of digital information from multiple sources, and in many different formats.
 - b) **STORE** – One or more storage containers to contain, evidential, non-evidential, archive, investigative, citizen provided and allow for movement between storage containers based on business requirements.
 - c) **CONSUME** – The ability for disparate Police systems to access and consume the information, both the original digital file and any associated metadata. This should be open API driven so that current and future Police systems are able to access this information as required.
- 2.2.5 Polices preference is for a building block driven system whereby components can be added and removed from the solution as required to meet business needs and to cater for the fast moving digital space.
- 2.2.6 Ability to cater for both evidential and non-evidential information.
- 2.2.7 Is device and media agnostic.
- 2.2.8 Has API's that can link information to Police Case Files and other systems
- 2.2.9 Digital by Default - applications and services are designed and built to be independent of and support multiple delivery channels.
- 2.2.10 Provides both analysis and artificial intelligence capability either inherently or able to connect via APIs to systems that do.
- 2.2.11 Accessible by the General Public, Police, partners and other Agencies.
- 2.2.12 Cloud based, although Police are not completely adverse to on premise and or hybrid configurations.
- 2.2.13 Easy to use.
- 2.2.14 Searchable.
- 2.2.15 Enables object detection.
- 2.2.16 Ability to migrate any existing data to the platform.
- 2.2.17 A business-oriented architecture.
- 2.2.18 Secure by design. Role based access controls and various levels of security classification should be catered for.
- 2.2.19 Manages data disposal.
- 2.2.20 Any solution will need to comply with at least the following New Zealand acts and regulations:
 - a. Evidential Regulations (2007)
 - b. Evidence Act (2006)
 - c. Criminal Disclosure Act (2008)
 - d. Criminal Procedure Act (2011)
 - e. Criminal Procedure Rules (2012)
 - f. Public Records Act (2005)

- 2.2.21 The solution would be expected to be highly available to meet the operational needs of Police, and without risk of data loss for information that is stored in the system.
- 2.2.22 The diagram below depicts at a high level what the Police Digital environment could look like, what tool sets would be required to manage and analyse this information, potential integration into Police internal “systems” and to other Government Agencies.

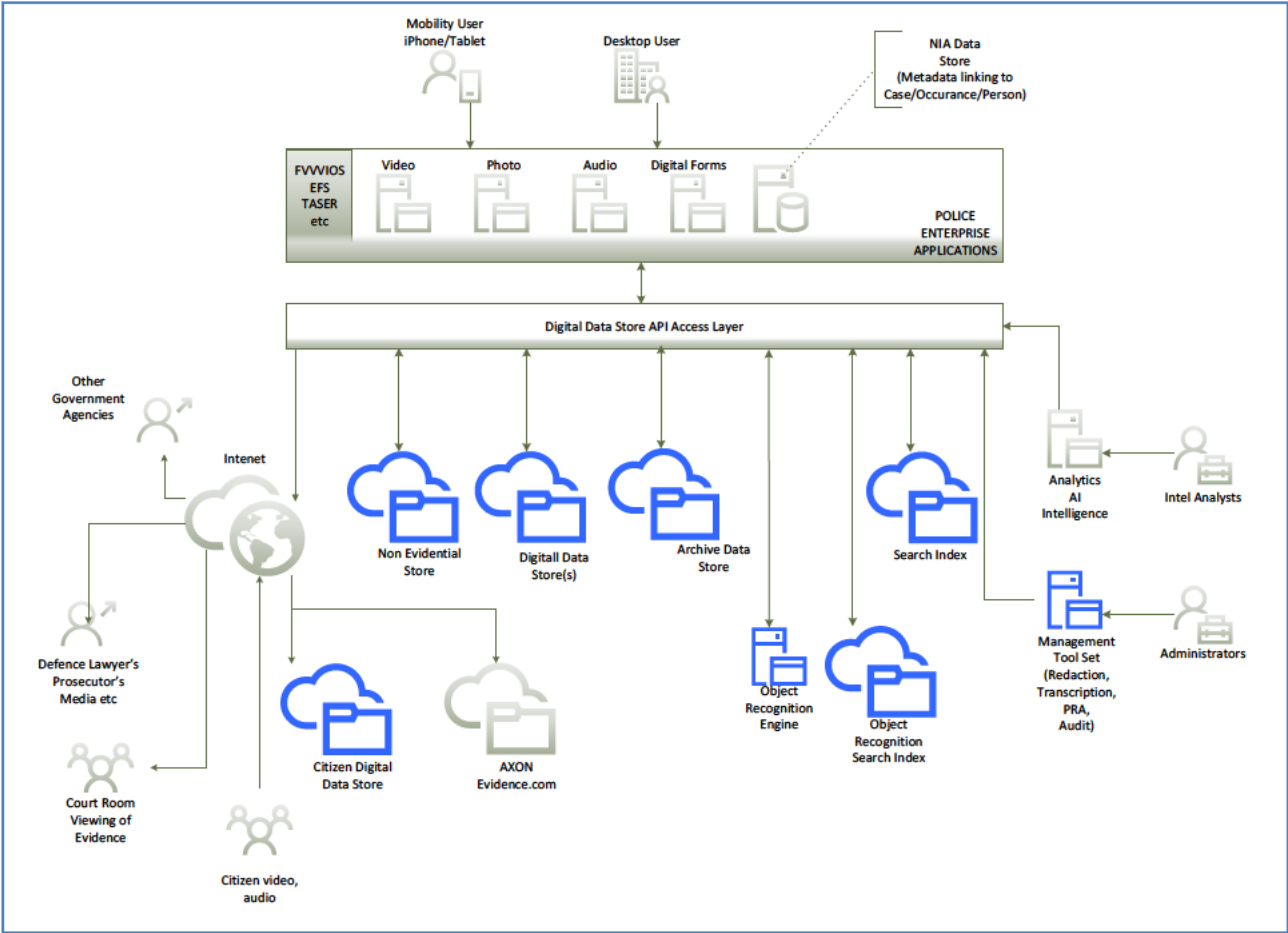


Table 1 – High Level Diagram of an envisioned Police Digital Information Environment

Appendix 1:

RFI Questions & Response Form

Please complete the Form below and return electronically to the email contact advised in Section 1.

1. Supplier's contact person for this RFI	
Contact person:	
Position:	
Phone number:	
Mobile number:	
Email address:	

2. Respondent's organisational profile	
Full legal name:	
Trading name: (if different)	if applicable
Name of parent company:	if applicable
Physical address:	for company, insert registered office
Location of head office:	city in New Zealand or if overseas, please specify city and country
Type of entity (legal status):	sole trader / partnership / limited liability company / other please specify
Size of organisation	Annual Sales Number of employees

3. Supplier's Response to RFI	
Question	Supplier's Response
Outline your companies' experience relating to digital data management. Focus on areas of particular strength that would benefit NZP.	
Provide a brief overview of your organisation's overall offerings (products and services) as they relate to digital data management. This should summarise your strengths, scale (i.e. number of customers and value), delivery capability and unique benefits relating to these offerings.	
In responding to this opportunity, will you	

represent any strategic partners or global supply relationships? If so, who and for what?	
Describe your Proposed Solution in technical terms and provide a statement of your capability.	
Brief Product / Solution description. (Product brochures / case studies may also be attached to your response to provide more information)	
Does your offering inherently provide management of evidence to the level required to meet legislation? If no, what would be required and how do you propose that would be established?	
Provide an overview of the integration capabilities of your API's	
Provide an overview of the capabilities of your object store.	
Provide an overview of the analysis and artificial intelligence capability be clear if this is inherent in the solution or will via API connections.	
Provide an overview of data disposal capabilities.	
Do you have any insights / key lessons learned from previous implementations as they relate to the specifics of digital data management?	
Explain why your proposed solution is a cost effective solution to manage digital data.	
How many customers use your product?	
What is your licensing model?	
Provide indicative Licensing Price Bands as per the licensing model above?	
Ongoing service costs per annum?	

Remotely Piloted Aircraft Systems (RPAS)

Table of Contents

Table of Contents	2
Policy statement and principles	3
What	3
Why	3
How	3
Overview	4
Introduct on	4
Types of RPAS	4
Purpose	4
Further nformat on	4
Police use of RPAS	5
When operat ng RPAS for Po ce operat ons	5
In-house capab ty (workgroups w th CAA cert fcat ons)	5
Tra n ng prov der	5
Other Government agenc es	5
Contracted prov ders	6
Legal authority and requirements	7
C v Av at on Act 1990	7
C v Av at on Ru es	7
Author ty for v sua surve ance	7
Operat on over pr vate property	7
Cr m na d sc osure	8
Storage and retent on of magery	8
Pr vacy cons derat ons	8
Complaints of public use of RPAS	10
Breach of C v Av at on Ru es on RPAS Use	10
Cr m na offences	10
Trespass	10
Pr vacy breaches	11
Countering the use of RPAS	12
Appendix 1 – Approved List of RPAS for In-house Operational Use	13
Appendix 2 – Approved List of Contracted Providers	14
Appendix 3 – Identifying the Privileges granted to a Part 102 certified Operator	16

Policy statement and principles

What

This chapter covers the PAS:

- operational use of RPAS by Police and for Police
- response and investigation of RPAS complaints
- countering the use of RPAS.

Why

To maintain public trust and confidence in Police:

- for operational use by Police, ensuring all use complies with relevant legislation and rules will contribute to trust and confidence
- responding to, and investigation of RPAS complaints appropriately, and in collaboration with CAA will contribute to trust and confidence
- as the risks of misuse of RPAS increase, counter RPAS methodologies will assist Police with managing this risk.

How

Operational use of RPAS will be through a range of options:

- In house capability where districts may operate RPAS
- Police workgroups with appropriate CAA certifications (pending)
- Other government agencies
- Contracted providers.

Response and investigation of RPAS complaints will be managed with CAA who has the primary responsibility for airspace safety.

Current technologies countering RPAS is in a developing phase and have varying degrees of effectiveness. There are also significant legislative constraints limiting the ability to deploy countering technologies.

Overview

Introduction

Remotely Piloted Aircraft Systems are also known as Unmanned Aerial Vehicles (UAVs), Unmanned Aircraft Systems (UAS) and drones.

These devices are becoming more commonplace globally. Advances in flight control technology and their low cost of operation make RPAS popular amongst hobbyists and provide a viable alternative to helicopters and fixed wing aircraft in many commercial situations.

Commercially, RPAS is proving to be an important tool with the ability not only of taking photographs but surveying, transportation and carrying a range of specialist camera systems and other payloads.

The use of RPAS by Police provides potential benefits, however it has a number of risks. The risks include RPAS losing control or crashing causing injury or damage to property or straying into controlled airspace as well as legal issues regarding privacy. Benefits include reduced costs for scene aerial imagery, mapping and surveillance of target addresses, as well as the ability to add value to the imagery by adding geographical information.

The protection of privacy is a key aspect to the successful use of RPAS as, where they are fitted with cameras, they will inadvertently capture imagery beyond the target location.

Suggested uses of RPAS include crime scene imaging, search and rescue, exhibit recording, serious road crash scene surveying, locating items of interest and providing enhanced situational awareness to tactical interventions and disasters to assist decision making. There will potentially be a wider range of benefits as technology develops.

Types of RPAS

Small rotary wing RPAS provide the ability to gain a view by climbing vertically, and manoeuvring over short distances, these are known as multi copters or quad copters. This platform provides a bird's eye view of a place, person, area or thing.

Small fixed wing RPAS (wingspans of up to approximately 3m) provide longer range, greater endurance (flight time) and the ability to search, photograph, video, or map a large area.

Purpose

This chapter:

- provides options on the use of RPAS to support policing operations
- provides guidelines on how Police will use RPAS when operating in house capability
- ensures that Police use of RPAS is safe, and complies with legislation including the Search and Surveillance Act 2012, Privacy Act 2020 and Civil Aviation Authority Rules
- outlines how Police handle complaints from members of the public where RPAS is involved
- provides guidance on countering RPAS misuse.

Further information

For all RPAS related information, contact Response and Operations at PNHQ on:

- E mail: rpas@police.govt.nz
- Telephone: Extn: 41133
- DDI: (04) 4704833

Police use of RPAS

RPAS provide Police with a potentially valuable tool. Technology advancements mean RPAS may add value to policing.

The options available to Police to use RPAS operationally are:

- in house capability where districts may operate RPAS, subject to approved training, qualifications and appropriate CAA certifications (pending);
- other government agencies; and
- contracted providers.

When operating RPAS for Police operations

- The RPAS must be of a make and model from the approved list (refer appendix one).
- The operator must have successfully completed the approved training or be under the direct supervision of a member who has completed this training.
- Must fly in accordance with the rules under Part 101 of the Civil Aviation Rules.
- Where, for any reason, the rules under Part 101 have been breached, must notify Response and Operations as soon as practicable via e mail: rpas@police.govt.nz.

The operator of the RPAS is the person responsible for ensuring the RPAS is operated safely and in accordance with all relevant legislation and rules.

In-house capability (workgroups with CAA certifications)

Work is currently underway for Police to obtain CAA certifications (Part 102) which will provide Police with specified “privileges” to operate outside some of the constraints of the Part 101 rules. The workgroups included in this work are:

- Photography Section
- Serious Crash Unit
- Tactical Groups Special Tactics Group and Armed Offenders Squad.
- Search and Rescue
- Surveillance.

This chapter will be updated once this certification is attained. The estimated timeframe for certification is fourth quarter of 2020.

Other workgroups can be included in this certification by making a request to Response and Operations.

Training provider

Police has approved Aviation Safety Management Systems Ltd (ASMS) as the single national training provider for RPAS training.

ASMS will provide all the training required for initial certification of pilots, as well as the additional training required by the (pending) Part 102 certification for:

- annual competency assessment;
- unshielded flight at night;
- exercise of advanced privileges such as Beyond Visual Line of Sight.

ASMS is also able to provide expert advice on the operation of RPAS within the broader legal framework that Police operate in, including the Search and Surveillance Act 2012.

Enquiries for training should be made directly to the National Manager: Response and Operations.

Other Government agencies

Many government agencies are developing their own RPAS capability.

An all of government forum for agencies developing RPAS capability meets regularly to collaborate on a range of issues, including policy, technologies and operating procedures. Agencies include:

- Fire and Emergency NZ (FENZ)

- NZ Defence Force (NZDF)
- Customs
- Ministry of Primary Industries (MPI)
- Civil Aviation Authority (CAA)
- ESR
- Corrections.

At present, FENZ has offered to operate RPAS for Police in geographical areas they operate. These areas include:

- Auckland
- Rotorua
- Hawkes Bay
- Wellington
- Christchurch.

Requests for FENZ assistance can be made through Comms. Requests will be considered by the FENZ RPAS programme manager.

For any questions on using other agencies, contact Response and Operations.

Contracted providers

Although Police has approved a list of contracted providers available to operate RPAS, these providers should only be used if no other capability is available.

A list of these contracted providers is contained in [Appendix Two](#).

Where contracted providers are engaged, they will provide advice to Police on any requirements they have to operate under their certifications.

Contracted providers must be supervised. Where operations involve search or surveillance then SASA requires that the contracted provider is supervised at all times by a constable (section [56](#)).

Any imagery requested by Police and collected by the contractor must be saved directly to an SD card which is provided to the supervising Officer at the conclusion of the operation/flight. Assurances must be obtained that any imagery related to an operation has been permanently deleted from the RPAS and associated flight controller, and that it has not been uploaded to an internet or “cloud” server.

For any questions or any issues on contracted providers, contact Response and Operations.

Legal authority and requirements

The use of RPAS in the Police context is subject to:

- [Civil Aviation Act 1990](#) and Civil Aviation Rules
- [Search and Surveillance Act 2012](#)
- [New Zealand Bill of Rights Act 1990](#)
- [Privacy Act 2020](#)
- [Criminal Disclosure Act 2008](#)
- [Surveillance by radar and from aircraft, drones, etc](#)

Civil Aviation Act 1990

The Civil Aviation Act 1990 provides the general legal framework for operation of any aircraft in New Zealand. The single most important provision for Police use of RPAS is the protection against trespass contained in section 97(2). That section provides that there is no action available in trespass so long as the height above ground at which the aircraft is operated is reasonable in the circumstances of the case, so long as the provisions of the Civil Aviation Act and the Civil Aviation Rules are complied with.

There have been several drug related prosecutions where the defendant claimed that the Police surveillance flights were an illegal search due to the aircraft trespassing in the airspace over the property. Compliance with applicable Civil Aviation Rules has been important to ensure that the trespass claim was dismissed.

Civil Aviation Rules

[Part 101](#) controls the use of gyrogliders and parasails, unmanned aircraft (including balloons), kites and rockets, which are under 25kg. To comply with Part 101, operators must:

- not operate an aircraft 25kg or larger and always ensure that it is safe to operate
- at all times take all practicable steps to minimise hazards to persons, property and other aircraft
- fly only in daylight unless shielded operation or indoors
- give way to all crewed aircraft
- be able to see the aircraft with own eye at all times
- not fly higher than 120 metres above ground level (exceptions exist)
- have knowledge of airspace restrictions in force
- when flying in controlled airspace, obtain air traffic control clearance
- not fly in special use airspace without permission of the controlling authority
- have consent from anyone below the aircraft
- have consent of the property owner or person in charge of the area being flown above (exceptions apply)
- not operate within 4 km of an aerodrome (as operators will have completed the necessary training, there is an exception to this rule).

Once Part 102 certification has been obtained, there will be “privileges” for approved Police pilots to operate outside some of the above restrictions.

Authority for visual surveillance

The Search and Surveillance Act 2012 (SASA) provides the ability to undertake visual surveillance of private activity in private premises or in the curtilage of a dwelling in order to obtain evidential material. If the RPAS to be used with a visual surveillance device to gather evidential material, check first whether the activity is permitted under SASA, and whether a surveillance device warrant is required (see section [46](#)).

Note: In some situations of emergency or urgency a warrant is not required to be obtained (see section [48](#)).

Once a surveillance device warrant is issued, or emergency powers are used, lawful surveillance can be carried out in accordance with the warrant or emergency power. A contractor engaged by Police may carry out activities authorised by the warrant on behalf of Police provided the contractor remains, at all times, under the supervision of a constable (section [56](#)).

Operation over private property

Authority for operation over private property is very limited for operations conducted under Part 101.

The Part 101 rules require that permission is obtained from the owner or occupier of any property overflown. Those rules do not define what is meant by “occupier”. It can be argued that where Police have a legislative authority to occupy a property (for example a search warrant) then, as a temporary occupier, Police may authorise the use of RPAS over that property. However, this right is not certain, and could be challenged in court proceedings. This exception only applies to a property Police have a legislative authority to occupy and not neighbouring properties.

Under (pending) Part 102 certification there will be a broader scope for operation over private property without obtaining prior consent from the owner or occupier.

In all cases it is up to the operator to ensure any potential hazards for operating the RPAS in that area are identified and considered.

Criminal disclosure

Section [13](#) of the Criminal Disclosure Act 2008 Act requires full disclosure of relevant information held by Police to the defendant including rebuttal information. The defendant may also request additional disclosure under section [14](#). Disclosure under both provisions is only required if the information or exhibit is “relevant” as defined in the Criminal Disclosure Act, namely “tends to support or rebut, or has a material bearing on, the case against the defendant.”

Imagery from private premises or of individuals that is not “relevant” to the criminal case should not be released as this may compromise the privacy of individuals not associated with the case.

Check the Police instructions on [criminal disclosure](#) when deciding what information to disclose or withhold.

Storage and retention of imagery

This section covering the storage and retention of imagery applies to all RPAS use by Police, whether in house, other agencies or contracted providers. This section should be read in conjunction with the ‘[Police filming and audio recording of operations and events](#)’ chapter.

It is simple to capture high resolution imagery and video when using RPAS. There are implications for the ease of transferring, storage and use of such large digital media files. Thought should be given to the lifecycle of the photos and videos captured on RPAS to avoid unnecessary time and costs associated with their processing and storage.

Security and integrity are key principles when dealing with any imagery captured by Police. Imagery captured from RPAS using third parties contracted by Police must:

- be recorded on removable storage systems (e.g. SD cards, flash drives, etc.)
- be handed over to Police immediately following completion of capturing imagery
- not be held by third parties or other copies made by the contractor
- be assigned an exhibit number
- be forwarded to Forensic Photography for storage and management in accordance with the ‘[Police filming and audio recording of operations and events](#)’ chapter.

SASA sets out time frames for retaining and then disposing of raw surveillance data obtained under the SASA. Note that once all Court proceedings have finished or after three years, all raw surveillance data, excerpts from raw surveillance data, and information obtained from it must be deleted or erased unless a Judge makes an order extending the period for retaining it.

See also ‘Privacy considerations’ (next below).

Privacy considerations

The issue of privacy when using RPAS is real. Most high resolution cameras used on RPAS flights will inadvertently collect imagery, including personal information, outside the target address and within the curtilage of private premises.

A variety of statutes allow and control the manner in which Police may collect evidence for court or resolve emergency situations; yet at the same time Police must be cognisant of, and comply with, the requirements to protect the privacy of individuals outside the focus of their operation. Care must be taken to avoid the inadvertent capture of images that are not relevant to the target, whether on private premises or not.

To comply with the Privacy Act, when using RPAS it is important to remember the key Information Privacy Principles

summarised here from the Privacy Commissioner's website, with some practical guidance:

- **Only collect information you need:** take care in the deployment of [RPAS] to avoid viewing or capturing imagery outside the target location.
- **Tell people about what you are doing:** Where a [RPAS] is used on a pre planned operation, where practicable, Police should notify people in the area observed of the operation.
- **Control access to personal information:** keep the information gathered via the [RPAS] secure.
- **Once you no longer need the personal information for the reason you collected it dispose of it securely so that no-one can retrieve it:** If the use of the visual surveillance device via RPAS is pursuant to the Search and Surveillance Act 2012, deal with evidence in the manner required under that Act. In all other cases, information should be deleted as soon as it is not needed for the purpose it was collected.

The 2012 Practice Note for Hearing of Applications for Surveillance Device Warrants requires any applications for use of a visual surveillance device warrant to set out the procedures to be adopted to keep private, images not required for the purposes of the investigation.

Complaints of public use of RPAS

Breach of Civil Aviation Rules on RPAS Use

The rules governing the use of RPAS are contained in the [Civil Aviation Rules](#). The Civil Aviation Authority (CAA) has the responsibility for ensuring compliance with those rules.

[Part 101](#) controls the use of gyrogliders and parasails, unmanned aircraft (including balloons), kites and rockets, which are under 25kg. To comply with Part 101, operators must:

- not operate an aircraft 25kg or larger and always ensure that it is safe to operate
- at all times take all practicable steps to minimise hazards to persons, property and other aircraft
- fly only in daylight unless shielded operation or indoors
- give way to all crewed aircraft
- be able to see the aircraft with own eye at all times
- not fly higher than 120 metres above ground level (exceptions exist)
- have knowledge of airspace restrictions in force
- when flying in controlled airspace, obtain air traffic control clearance
- not fly in special use airspace without permission of the controlling authority
- have consent from anyone below the aircraft
- have consent of the property owner or person in charge of the area being flown above
- not operate within 4 km of an aerodrome (exceptions exist).

An operator will require an unmanned aircraft operator certificate (UAOC) issued under [Part 102](#) if the operator intends to operate an unmanned aircraft and cannot operate strictly within the limitations of Part 101. Certification as an Unmanned Aircraft Operator must be first obtained from the CAA under Part 102. Certified operators are listed on the CAA website for public view although the scope of their authorised operations is not listed there. However, the scope of authorised operations (“privileges”) can be established from the “Operations Specifications” that CAA issues to the operator more information on this is provided in Appendix 3.

CAA is primarily responsible for ensuring compliance with the rules to keep airspace safe. Where there has been a breach or suspected breach of these rules, complaints can be directed to CAA via:

- Telephone: (04) 5609480
- E mail: info@caa.govt.nz

Where the rule breach presents a risk to safety or a significant impact, Police should respond to attempt to identify the operator. Where the operator is identified, Police can liaise with CAA to determine the best course of action to deal with the incident.

Criminal offences

Where a criminal offence has been committed or suspected of having been committed using an RPAS, a complaint should be taken and liaison with CAA to establish what action should be taken. Examples include using an RPAS to record intimate images or intimidating others.

Where Police undertake an investigation where an RPAS has been used or suspected of being used, CAA can assist with subject matter expertise and should deal with any CAA regulatory or rule breach while police deal with any criminal investigation.

Trespass

An operator flying under Part 101 will be committing trespass if they are flying over a property where they do not have permission to fly. This includes flight over Department of Conservation land.

An operator flying under Part 102 will also be committing trespass if they either (a) do not have the privilege to fly over third party property, or (b) do not comply with the terms of that privilege. (How to establish the privileges held by a certified operator is provided in [Appendix 3](#)).

If trespass is committed with an RPAS then the normal provisions of the Trespass Act 1980 can be applied as well as breach of the CAA Part 101 rules.

Privacy breaches

The Privacy Commissioner can also receive and investigate complaints of a breach of privacy.

Countering the use of RPAS

RPAS have the potential to be used criminally and misused to cause harm. There have been recorded incidents in New Zealand where RPAS have been used by criminals to observe Police.

Systems to counter the use of RPAS are developing. These systems are designed to detect RPAS and take control or otherwise prevent them from flying.

At present there are no systems sufficiently effective enough and these technologies will continue to be monitored for effectiveness.

There are also several legislative impediments to the use of technologies for countering RPAS.

The Aviation Crimes Act 1972 prohibits the destruction of an aircraft in service, and also prohibits actions causing “damage to an aircraft in service which renders the aircraft incapable of flight or which is likely to endanger the safety of the aircraft in flight”. An RPAS is an aircraft, so these provisions apply to all actions taken against RPAS.

The Radiocommunications Regulations (Prohibited Equipment – Radio Jammer Equipment) Notice 2011 prohibits the use of radio jamming equipment. Only the Department of Corrections currently has a licence to use jammers, and that is subject to strict controls.

In addition to the above, any counter RPAS system that would take control of the drone while it is in flight potentially contravenes the prohibition against interfering with a computer system contained in section 250 of the Crimes Act 1961.

Appendix 1 – Approved List of RPAS for In-house Operational Use

- DJI Mavic range
- DJI Spark
- DJI Phantom range (Phantom 4 and above)
- DJI Matrice range

Districts must notify National Manager: Response and Operations if intending to purchase a RPAS capability.

[illegible]

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16
17	18	19	20
21	22	23	24
25	26	27	28
29	30	31	32
33	34	35	36
37	38	39	40
41	42	43	44
45	46	47	48
49	50	51	52
53	54	55	56
57	58	59	60
61	62	63	64
65	66	67	68
69	70	71	72
73	74	75	76
77	78	79	80
81	82	83	84
85	86	87	88
89	90	91	92
93	94	95	96
97	98	99	100

Appendix 3 – Identifying the Privileges granted to a Part 102 certified Operator

Whether a Part 102 certified operator listed in [Appendix 2](#) is utilised as a contractor, or a Part 102 certificated operator is the subject of investigation, the documentation issued by the Civil Aviation Authority (CAA) to that operator will identify what “privileges” the CAA has granted.

Ask the UAS operator for a copy of their Part 102 certificate and the associated document called the “Operations Specifications”. The top of the first page of the Operations Specifications is shown below. If the UAS operator cannot show you this document then there is no evidence that CAA has granted them any particular privileges, and they should be required to comply with the rules prohibiting flight over people and property.



Part 102 Unmanned Aircraft Operations Specifications *Sample Company Ltd*

This Specification forms part of Certificate No. UAOC12345 granted pursuant to CAR Part 102.

1. Location of the Principal Base of Operation

As shown below, the bottom of the last page of the Operations Specifications has a section called “Additional Conditions”. Look for a condition that states “Operations pursuant to Rule 101.207 Airspace”. This condition will state the specific sections of the UAS operator’s “company exposition” (manual of procedures) and SOPs that specify the exact procedures and conditions that CAA has agreed to.

9. Additional Conditions

1. The holder of this certificate shall comply with the following identified rules:

Rule Part 12

2. Sample Company Ltd are to comply with Civil Aviation Rule Part 101 except where privileges are granted under this certificate.
 3. The aircraft must have an indelible label that can be viewed without removal of any covers, clearly identifying who the operator is.
 4. Operations pursuant to Rule 101.205 Aerodromes, specifically 101.205(a)(1)(i) must be conducted in accordance with the requirements of the company exposition, section 6.7 and associated SOP's.
 5. Operations pursuant to Rule 101.207 Airspace, specifically 101.207 (a)(1)(i) and (ii) must be conducted in accordance with the requirements of the company exposition, section 6.4 and associated SOP's.
 5. Operations pursuant to Rule 101.211 Night Operations must be conducted in accordance with the requirements of the company exposition, section 6.9 and associated SOP's.
- The current exposition is revision 0 , dated 17 August, 2017

Version number: 3

Owner: NM: Response &
Operations

Publication date: 07/12/2020

Last modified: 07/12/2020

Review date: 07/12/2025

Printed on : 07/12/2020

Printed from : http://tenone.police.govt.nz/pi/remotely_piloted_aircraft_systems_rpas