NEW ZEALAND POLICE
Ngā Pirihimana o Aotearoa

22 February 2021

Andrew Chen
By email to: fyi-request-13898-e7b0e854@requests.fyi.org.nz

Dear Dr Chen

OFFICIAL INFORMATION REQUEST – OUR REFERENCE: IR-01-20-37182

I refer to your Official Information Act (OIA) request, submitted via the FYI website on 8 December 2020, seeking information about the use of facial recognition technologies since mid-October 2017.

Following a recent telephone discussion with Police's Manager: Forensic Services, you refined the scope of your request, and in your email dated 2 February 2021 you confirmed: *"I'm interested in discussions that Police have had around adopting the use of facial recognition technologies, in particular whether privacy and ethics considerations have been taken into account, so documents like Privacy Impact Assessments would be of particular relevance."*

The refined scope of your request has been considered in accordance with the OIA and I am now able to respond as follows.

Police has given consideration to use of facial recognition technologies in the context of procurement in relation to ABIS2, which was required to support matching of static (i.e., not live streamed) suspect images against Police-held forensic photo collections, and in the circumstances surrounding the non-operational 'test' of Clearview AI, with which I gather you are already familiar. The relevant documents are already public, having been released by Police last year in accordance with our commitment to be transparent about the trial and use of new technologies. Those documents include the Privacy Impact Assessment (PIA) on ABIS2, the new policy on Proposals to test or trial use of emergent technology, and the Assurance Review on emergent technologies. In addition, procurement documentation relating to ABIS2, including detailed requirements and Request for Proposals documents, which have previously been released under the OIA, are attached.

You have asked specifically about how Police is taking relevant privacy and ethical considerations into account. In respect of facial recognition technology, a PIA on ABIS2 (linked above) was completed. More generally, technology acquisitions and proposals are subject to requirements for governance approvals and compliance with procurement processes, as appropriate to the nature and scale of the project. These processes by their nature routinely canvas legal, policy, privacy, and security issues; and may lead to more formal privacy analyses and/or security risk assessments.

Police National Headquarters
180 Molesworth Street. PO Box 3017, Wellington 6140, New Zealand.
Telephone: 04 474 9499. Fax: 04 498 7400. www.police.govt.nz

The July 2020 Assurance Review's findings and recommendations nevertheless reflect that more can be done to systematise internal oversight and external stakeholder engagement on privacy and related issues, particularly in respect of emergent technologies.

As you will be aware, and as we have discussed previously, Police's response to those findings has included introduction of the new policy (also linked above), and a commitment to establishing an independent expert panel to review new technology proposals. A process to establish that expert panel is well underway. Police has also signed up to the *Algorithm Charter for Aotearoa New Zealand*. These are significant steps towards improving our ability to provide public transparency and assurance that privacy and ethical concerns are identified, fully considered, and appropriately weighed before a decision is made whether or not to introduce an emergent technology.

As also discussed when we met last month, I am continuing to liaise with the office of Deputy Chief Executive Mark Evans to identify an opportunity for you to meet with him directly. That meeting may provide a further opportunity for you to explore Police's organisational thinking and approach to these questions. I hope to soon be able to propose a time, within the next few weeks, for that meeting to take place.

In closing, once again please accept my apologies for the length of time taken to respond to this request; and I trust, despite the delay, the information provided is helpful. However, if you are dissatisfied with this response, you may ask the Office of the Ombudsman to investigate and review Police's handling of your request.

Respectfully

Mike Webb
Director: Assurance

New Zealand Police
Request for Proposals
ABIS 2
(Automated Biometric Identification Solution)

TN18/03

RFP released: 15 January 2018

Deadline for Questions: 5pm 23 February 2018

Deadline for Proposals: 12noon 8 March 2018

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

Contents

This opportunity in a nutshell

New Zealand Police (Police) is seeking an integrated biometric technology solution to support multi-modal capabilities, including:

- A photo database able to import, store and search facial images in separate categories; such as Suspect (unknown id), Prisoner/Arrestee, Firearms Licences, Missing Persons, Individuals included in Child Sex Offender Register (CSO) ,
- Capability to electronically produce photo montages and photo books,
- Facial recognition technology capable of searching external facial images (eg CCTV images) against the facial images database and search images within the database against other images within the database.
- Using existing Livescan technology, capture, store, classify and search scars, marks and tattoo (SMT) images (in separate categories including; Suspect (unknown id), Prisoner/Arrestee, Missing Persons).
- Capture, store and search images and descriptions of clothing.

What we need

Police want to link the facial image management system, a Scars, Marks and Tattoos system(s),and clothing system to the existing overall process for electronic biometric capture within station/sites (including the LiveScan [Fingerprints/face capture] process) to provide a fully integrated biometric image-to-image system.

The key business driver for this Project is a 'base' product to replace the existing image management system functionality and supplementary products including:

- The replacement of the photo database
- The replacement facial recognition technology
- the introduction of an image based scar, mark and tattoo database, with capture, classify and search capability (considering manual and automated searching), for prisoner scars, marks and tattoos captured at the time of charge using existing Livescan technology
- the introduction of a soft biometric system with the capability for direct scar, mark and tattoo database comparison with CCTV or in relation to victim identification
- the introduction of an image based clothing database captured during an investigation, with capture, classify and search capability
- the introduction of a system with the capability to classify and search clothing descriptions for intelligence purposes.

Background

The existing image management system (Photo Manager) was fully implemented by Police in 2009 to replace the Photographic Image Management System (PIMS) which was a standalone system implemented by Police in 1992. The image management system has provided a single repository for all identification

images including Formal Prisoner Photographs, Firearms Licence holders, Suspect images and Missing Persons images but has limited facial recognition capability.

Currently scar, marks and tattoo details are held in a coded/textural format and the current clothing description database is held as a spreadsheet format. There are no image based capabilities to capture, classify and search soft biometrics; scars, marks and tattoos for biometric identification or classify and search clothing images for intelligence purposes.

What we don't want

Police is not seeking theoretical Proposals relating to systems at research and development stage.

What's important to us?

Police is seeking a reputable supplier who can demonstrate its ability (capability, experience and infrastructure) to deliver a product fit for purpose, not only meeting Police's current needs but also with capability for the future.

The supplier involved in the delivery will have a proven track record in delivering similar systems to government organisations and the personnel involved in the delivery will hold relevant qualifications and have experience in delivering such systems.

There is an expectation that the requirements will be delivered in full, on time, to specification and within budget.

Why should you bid?

This provides a unique opportunity for an organisation to provide an innovative mobile and desktop forensic capability solution(s) with the capability to link/identify individuals from images captured and/or stored by Police.

A bit about us

Police is the lead agency responsible for reducing crime and enhancing community safety in New Zealand, we provide policing services 24 hours a day, by land, sea and air. We respond to more than 860,000 emergency calls and one million non-emergency calls each year.

Police employ over 12,000 staff spread through 12 Police Districts

Mobility is a fundamental enabler for New Zealand Police to deliver "Our Business". Since the rollout of tablets and smartphones began in 2013 as part of Policing Excellence, Mobility has revolutionized the way New Zealand Police operates, ensuring it is one of the most mobile fleets in the world.

SECTION 1: Key information

1.1 Context

a. This Request for Proposal (RFP) is an invitation to suitably qualified suppliers to submit a Proposal for the ABIS 2 (Automated Biometric Identification Solution) Facial Image Identification and Management, Scar, Mark and Tattoo, and Clothing database Technology Solution(s) (From here referred to as ABIS 2)

b. This RFP is a single-step procurement process.

c. Words and phrases that have a special meaning are shown by the use of capitals e.g. Respondent, which means '*a person, organisation, business or other entity that submits a Proposal in response to the RFP. The term Respondent includes its officers, employees, contractors, consultants, agents and representatives. The term Respondent differs from a supplier, which is any other business in the market place that does not submit a Proposal.*'. Definitions are at the end of Section 6.

1.2 Our timeline

a. Here is our indicative timeline for this RFP.

Steps in RFP process:	**Date:**
Deadline for Questions from suppliers:	5pm 23/02/18
Deadline for the Police to answer suppliers' questions:	02/03/18
Date of the supplier briefing sessions:	22 - 26/01/18
Deadline for Proposals:	12 noon 08/03/18
Shortlisted Respondents' presentations:	week starting 09/04/18
Unsuccessful Respondents notified of award of Contract:	11/05/18
Respondents' debriefs:	week starting 21/05/18
Anticipated Contract start date:	Quarter 3 2018

b. All dates and times are dates and times in New Zealand.

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 Proposal.

c. If you would like to attend our supplier briefing session please email our Point of Contact to register.

d. **Our Point of Contact**

Title/role: Contracts Administrator

Email address: tenders.national@police.govt.nz

1.4 Developing and submitting your Proposal

- This is an open, competitive tender process. The RFP sets out the step-by-step process and conditions that apply.
- Take time to read and understand the RFP. In particular:
  i. develop a strong understanding of our Requirements detailed in Section 2.
  ii. in structuring your Proposal consider how it will be evaluated. Section 3 describes our Evaluation Approach.

- For helpful hints on tendering and access to a supplier resource centre go to: www.procurement.govt.nz / for suppliers.
- 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.
- There is also an opportunity for Respondents to register for an individual briefing session with members of the Project team during the week 22-26 January. The briefing session is for 90 minutes and is designed as an interactive session providing an opportunity for Respondents to gain a deeper understanding of the Police environment, the required solution, and how they may best meet Police requirements. The briefing session is optional and can be provided by teleconference. Should you wish to book a briefing session please Email our Point of Contact.
- In submitting your Proposal you must use the Response Forms provided. There are three response forms you must complete;
    - RFP Response form (which provides your corporate information, referees etc.)
    - Requirements Response form (which details how your solution will meet all of the requirements)
    - Price Response form
- You must also complete and sign the declaration at the end of the RFP Response Form.
- Proposals must be submitted in two separate files knows as the 'Two Envelope System':
    - File 1: the response to the requirements
    - File 2: all pricing information
- No pricing information is to be contained in File 1.
- Check you have provided all information requested, and in the format and order asked for.
- Having done the work don't be late – please ensure you get your Proposal to us before the Deadline for Proposals!

1.5 Address for submitting your Proposal

a. Proposals must be submitted on a USB stick accompanied by one signed original hardcopy to the following address:

RFP TN18/03 ABIS 2

Police National Headquarters

180 Molesworth Street, Thorndon

Wellington

Attn: Contracts Administrator

1.6 Our RFP Process, Terms and Conditions

a. **Offer Validity Period**: In submitting a Proposal the Respondent agrees that their offer will remain open for acceptance by the Buyer for six calendar months from the Deadline for Proposals.

b. The RFP is subject to the RFP Process, Terms and Conditions (shortened to RFP-Terms) described in Section 6. We have made the following variation/s to the RFP-Terms:

   i. Section 6 paragraph 6.10(a) is deleted in its entirety and replaced with the following: 'At any time after selecting a Successful Respondent(s), the Buyer will offer all Respondents who have not been successful a debrief. When a Respondent requests a debrief, the Buyer will provide the debrief within 30 Business Days of the date of the request, or of the date the Contract is signed, whichever is later.'

   ii. Section 6 paragraph 6.21(a)(iv) is deleted in its entirety. NZ Police intends to follow the stipulated evaluation process, but reserves the right to amend its approach.

1.7 Later changes to the RFP or RFP process

a. If, after publishing the RFP, we need to change anything about the RFP, or RFP process, or want to provide suppliers with additional information we will let all suppliers know by sending notifications of any changes to the registered contact by email.

SECTION 2: Our Requirements

2.1 Background

This section provides an overview of the requirements, Respondents are directed to the attached Detailed Requirements Document for further information.

This procurement relates to the delivery of an integrated biometric technology solution to support multi-modal capabilities, including:

- A photo database able to import, store and search facial images in separate categories; such as Suspect (unknown id), Prisoner/Arrestee, Firearms Licences, Missing Persons, Individuals included in Child Sex Offender Register (CSO)
- Capability to electronically produce photo montages and photo books
- Facial recognition technology capable of searching external facial images (eg CCTV images) against the facial images database and search images within the database against other images within the database.
- Using existing Livescan technology, capture, store, classify and search scars, marks and tattoo (SMT) images (in separate categories including; Suspect (unknown id), Prisoner/Arrestee, Missing Persons).
- Capture, store and search images and descriptions of clothing.

The existing facial image management system (Photo Manager) was fully implemented by Police in 2009 to replace the Photographic Image Management System (PIMS) which was a standalone system implemented by Police in 1992. The image management system has provided a single repository for all identification images including Formal Prisoner Photographs, Firearms Licence holders, Suspect images and Missing Persons images but has limited facial recognition capability. Currently scars, marks and tattoo details are held in a coded/textural format. There is no image based capability to capture, classify and search soft biometrics; scars, marks and tattoos for biometric identification. Information relating to a clothing type database is held on a standalone system in Auckland Metro Districts.

Going forward we wish to link the image management system, a Scars, Marks and Tattoos system(s),and clothing system to the existing overall process for electronic biometric capture within station/sites (involving LiveScan [Fingerprints/face capture] process), to provide a fully integrated biometric image-to-image system.

2.2 What we are buying and why

This RFP relates to the purchase of a 'base' product(s) to replace the existing image management system functionality and supplementary products including:

- The replacement of the photo database
- The replacement of facial recognition biometrics
- The introduction of image based scar, mark and tattoo database, with capture, classify and search capability, for prisoner scars, marks and tattoos captured at the time of charge using the existing Livescan technology

- The introduction of a soft biometric system with the capability for direct scar, mark and tattoo database comparison with CCTV or in relation to victim identification
- The introduction of image based clothing database, with capture, classify and search capability, for clothing

The key outcomes that we want to achieve are:

- Reduce time taken to provide forensic intelligence to investigators to support the identification and apprehension of suspects and the reduction of victimisations.
- Increase identifications of victims and suspects based on biometric information.
- Increase the quality and quantum of identifying particulars captured.

2.3 What we require: the solution

We are seeking a technology solution(s) to support the future state process and must provide a standardised national system that will provide a single source repository with the ability to store and manage:

- Facial images (in separate categories including; Suspect (unknown id), Prisoner/Arrestee, Firearms Licences, Missing Persons)
- Scars, marks and tattoo (SMT) images (in separate categories including; Suspect (unknown id), Prisoner/Arrestee, Missing Persons)
- Clothing images

The solution(s) must provide the following capability:

- Import, storage and management of facial images captured by Police from various sources
- Import, classify, storage and search of SMT images captured by Police from various sources
- Import, classify, storage and search of clothing images captured by Police from various sources
- Interface in real-time to NZ Police operational applications.

The following Functional Requirements are required:

- Import and storage of facial images captured within multiple business processes
- Import, classify and storage of SMT images captured within multiple business processes
- Import, classify and storage of clothing images captured within multiple business processes
- Management of stored facial, SMT and clothing images
- Interface to NZ Police's operational applications (including but not limited to National Intelligence Application (NIA)) for retrieval of personal attributes related to an image.
- Search and retrieve facial, SMT and clothing images using text based attribute searching.
- Enable the use of advanced suspect identification using facial recognition and SMT recognition (biometric identification)
- Enable the use of advanced intelligence using clothing data.
- Enable the production of Photo Books to allow the classification of photos by type.
- Enable the provision for evidential purposes a mechanism to produce Formal Photo Line-ups (Photo Montages) using Prisoner /Arrestee Photos. This will include the capability to interface with NZ Police operational application (OnDuty) which would manage the mobile user's need

within a single integrated application. The objective is for police to be able to show a witness a series of photographs on their mobility device in the future.

- Generate a file for new and renewed Firearms Licence details and an associated image for production of Firearms Licences (Licences are produced by an external supplier).
- Meet American National Standards Institute / National Institute of Standards and Technology (ANSI/NIST) minimum standard

The following are the Non-functional Requirements:

- NZ Police Administrator able to grant access authorisation to staff
- Ability to control access (e.g. read / write / delete) by user or group
- Full audit trail of all user transactions - all transactions will be date and time stamped
- Interfaces with NZ Police operational applications and third party solutions and environments
- Matches NZ Police operational applications availability conditions of 24/7 access
- Users accessing the system within the NZ Police network will be authenticated against Active Directory
- Application data archiving to provide the ability to view history log of changes to biometric data and audit reports
- Terminology consistent with that used by staff
- Online help
- Error logging

2.4 What we require: capacity

We are seeking suppliers that are able to demonstrate the capacity to deliver the requirements.

2.5 What we require: capability

We are seeking suppliers that are able to demonstrate the capability to deliver the requirements.

2.6 Contract term and management

We anticipate that the Contract will commence in Quarter 3 2018. The anticipated Contract term and options to extend are:

Description	Years
Initial term of the Contract	Five years
Options to extend the Contract	up to two extensions of two years each i.e. 5+2+2]
Maximum term of the Contract	Nine years

Each party will nominate both a Business Representative (day-to-day business and SLA adherence) and Relationship Manager (strategic and relationship development) to manage the contract lifecycle and its deliverables.

Appropriate SLAs will be agreed with the Successful Respondent and detailed in a schedule to the final Contract.

2.7 Key outcomes

The key deliverables and milestones through the delivery phase of the project will be agreed with the successful Respondent as part of the contract negotiations and implementation planning.

2.8 Other information

a. It is anticipated that Payment will be on successful delivery of milestones throughout the delivery phase of the project, a detailed schedule will be agreed with the successful Respondent

b. New Intellectual Property arising as a result of the Contract will be subject to Clause 15 of the Master Services Agreement provided with this RFP

2.9 Other tender documents

In addition to this RFP we refer to the following documents have been provided with this RFP These documents form part of this RFP.

1 ABIS 2 RFP Detailed Requirements Document

2 Master ICT Services and Deliverables Agreement

3 RFP Response Form

4 Requirements Response Form

5 Price Response Form

SECTION 3: Our Evaluation Approach

This section sets out the Evaluation Approach that will be used to assess Proposals.

3.1 Evaluation model

The evaluation model that will be used is weighted attribute (weighted criteria). Price is a weighted criteria and will be evaluated on the Total Cost of Ownership over the whole-of-life of the Contract.

There are no specific preconditions relating to this RFP however Respondents should note that there are multiple Mandatory Requirements for the solution detailed in the attached Detailed Requirements Document. Respondents should familiarize themselves with the Mandatory aspects of the solution when considering a response to this RFP.

A 'two envelope' system will be used for the evaluation. This means that Respondents must provide all financial information relating to price, expenses and costs in a separate sealed envelope/soft copy folder. The evaluation panel will firstly score each Proposal based on the weighted criteria listed below. Proposals will then be ranked according to their scores. Following completion of the scoring the sealed envelopes containing financial information will be presented to the panel. The panel will then assess which Proposals to shortlist based on best value-for-money over the whole-of-life of the Contract i.e. the scores and the total costs over the whole-of-life of the Contract.

3.2 Evaluation criteria

Proposals will be evaluated on their merits according to the following evaluation criteria and weightings.

Criterion	Weightings		
	Level 1	Level 2	Level 3
NON PRICE CRITERIA	**70%**		
Technical merit (fit for purpose) – degree in which good/services meet or exceed requirements		**60%**	
IMS			**50%**
Facial Recognition			**25%**
SMT/Clothing logo symbol			**25%**
Capability and Capacity of the supplier to deliver		**20%**	
Understanding of requirements			**20%**
Track record in delivering similar systems			**20%**
Operational and financial systems to manage delivery			**20%**
Process/methodology			**20%**
Project Management			**20%**
Other Benefits		**20%**	
Support			**50%**

Training			50%
PRICE CRITERIA	**30%**		
Total Cost of Ownership		**100%**	
Total weightings	**100%**		

3.3 Scoring

The following scoring scale will be used in evaluating Proposals. Scores by individual panel members may be modified through a moderation process across the whole evaluation panel.

Score	Explanation
0	No answer provided or totally non-compliant. (Non-Conforming)
1	The answer is substantially non-compliant. (Non-Conforming)
2	The answer is partially non-compliant. (Non-Conforming)
3	The answer has minor non-compliance. (Conforming)
4	The answer conveys compliance but lacks credible substantiation and/or cost transparency.
5	The answer conveys compliance with credible substantiation. May also include minor enhancements to the compliance/requirement.
6	The answer conveys an ability to exceed the required compliance with good benefits to NZ Police but will require formal confirmation of such to maintain score given.
7	The answer demonstrably exceeds the required compliance to a moderate extent, and provides moderate benefits/innovation relevant to NZ Police and reflects sound understanding with clear benefits/innovation.
8	The answer, with demonstrable experience, exceeds the required compliance to a significant extent and provides significant benefits/innovation relevant to NZ Police.
9	The answer, with demonstrable experience, exceeds the required compliance to a substantial extent and provides substantial benefits/innovation relevant to NZ Police and reflects significant collaboration and proven experience in the provision of the requirement/s.
10	The answer, with demonstrable experience, exceeds the required compliance to an exceptional extent and provides exceptional benefits/innovation relevant to NZ Police and reflects substantial collaboration and proven experience in the provision of the requirements, or The tender requirement is unchanged from current deliverables and the answer being evaluated from an incumbent provider has been assessed by the panel as a fully compliant response to a contractor **change management criteria**.

3.4 Conforming Tenders

After evaluation of the weighted non price evaluation criteria, only conforming tenders will proceed to the assessment of price. A Conforming Tender is defined as follows:

A Conforming Tender means a tender that, after assessment:

a. Receives a weighted score for each non price criteria greater than or equal to 30% (a minor non-compliance) of the criteria weighting as follows:

Non Price Criteria Criteria Number and Description	Criteria Weighting	Conforming Tender Minimum Weighted Score (30% of criteria weighting)
1. Technical Merit	**60**	**18**
2. Capability and Capacity	**20**	**6**
3. Other Benefits	**20**	**6**

3.5 Price

We wish to obtain the best value-for-money over the whole-of-life of the Contract. This means achieving the right combination of fit for purpose, quality, on time delivery, quantity and price.

If a Respondent offers a price that is substantially lower than other Proposals (an abnormally low bid), the Buyer may seek to verify with the Respondent that the Respondent is capable of fully delivering all of the Requirements and meeting all of the conditions of the Proposed Contract for the price quoted. Price will be evaluated on a total cost of ownership (TCO) basis and weighted using a lowest conforming price (LCP) methodology.

3.6 Evaluation process and due diligence

In addition to the above, we will undertake the following process and due diligence in relation to shortlisted Respondents. The findings will be taken into account in the evaluation process.

a. reference check the Respondent organisation and named personnel

b. interview Respondents

c. request Respondents make a presentation and demonstrate elements of their proposed solution

d. undertake a Police check for all named personnel prior to contract implementation

3.7 Optional evaluation process and due diligence

In addition to the above, we may undertake the following process and due diligence in relation to shortlisted Respondents. The findings will be taken into account in the evaluation process. Should we decide to undertake any of these we will give shortlisted Respondents reasonable notice.

a. other checks against the Respondent e.g. Companies Office

b. arrange site-visits

c. test products

d. inspect audited accounts for the last three financial years

e. undertake a credit check

f. undertake a Police check for all named personnel

3.8 Implementation Business Case

The Police Capability Investment Board (PCIB) has approved the Initial Business Case for the ABIS 2 project. Following finalisation of the recommendations resulting from this RFP Process an Implementation Business Case will be submitted to PCIB. Execution of the final agreement and commencement of the delivery phase of the project are subject to the approval of the Implementation Business Case.

SECTION 4: Pricing information

4.1 Pricing information to be provided by respondents

Respondents are to provide their price as part of their Proposal. In submitting the Price the Respondent must meet the following:

a. Respondents are to use the pricing schedule template provided.

b. the pricing schedule is to show a breakdown of all costs, fees, expenses and charges associated with the full delivery of the Requirements over the whole-of-life of the Contract. Tenders are to state any pricing adjustment methods that will apply for the unit rates throughout the life of the contract. Tenders are to state any conditions/volumes or activities that will affect the unit rates throughout the life of the contract.

c. where the price, or part of the price, is based on fee rates, all rates are to be specified, either hourly or daily or both as required.

d. in preparing their Proposal, Respondents are to consider all risks, contingencies and other circumstances relating to the delivery of the Requirements and include adequate provision in the Proposal and pricing information to manage such risks and contingencies.

e. respondents are to document in their Proposal all assumptions and qualifications made about the delivery of the Requirements, including in the financial pricing information. Any assumption that the Buyer or a third party will incur any cost related to the delivery of the Requirements is to be stated, and the cost estimated if possible.

f. prices should be tendered in NZ$. Unless otherwise agreed, the Buyer will arrange contractual payments in NZ$.

g. where a Respondent has an alternative method of pricing (i.e. a pricing approach that is different to the pricing schedule) this can be submitted as an alternative pricing model. However, the Respondent must also submit a pricing schedule that conforms.

h. where two or more Respondents intend to lodge a joint or consortium Proposal the pricing schedule is to include all costs, fees, expenses and charges chargeable by all Respondents.

SECTION 5: Our Proposed Contract

5.1 Proposed Contract

The NZ Police Master ICT Services and Deliverables Agreement that we intend to use for the purchase and delivery of the Requirements is provided as an attachment to this RFP.

In submitting your Proposal you must let us know if there are terms or conditions in the Proposed Contract that would be a significant impediment to negotiating a successful contract between the parties. The Response Form contains a section for you to state your position.

SECTION 6: RFP Process, Terms and Conditions

Note to suppliers and Respondents

- In managing this procurement the Buyer will endeavour to act fairly and reasonably in all of its dealings with interested suppliers and Respondents, and to follow due process which is open and transparent.
- This section contains the government's standard RFP Process, Terms and Conditions (shortened to RFP-Terms) which apply to this procurement. Any variation to the RFP-Terms will be recorded in Section 1, paragraph 1.6. Check to see if any changes have been made for this RFP.
- Words and phrases that have a special meaning are shown by the use of capitals e.g. Respondent, which means *'a person, organisation, business or other entity that submits a Proposal in response to the RFP. The term Respondent includes its officers, employees, contractors, consultants, agents and representatives. The term Respondent differs from a supplier, which is any other business in the market place that does not submit a Proposal.'* Definitions are at the end of this section.
- If you have any questions about the RFP-Terms please email our Point of Contact.

Standard RFP process

Preparing and submitting a proposal

6.1 Preparing a Proposal

a. Respondents are to use the Response Form provided and include all information requested by the Buyer in relation to the RFP.

b. By submitting a Proposal the Respondent accepts that it is bound by the RFP Process, Terms and Conditions (RFP-Terms) contained in Section 6 (as varied by Section1, paragraph 1.6, if applicable).

c. Each Respondent will:

i. examine the RFP and any documents referenced in the RFP and any other information provided by the Buyer

ii. consider all risks, contingencies and other circumstances relating to the delivery of the Requirements and include adequate provision in its Proposal to manage such risks and contingencies

iii. document in its Proposal all assumptions and qualifications made about the delivery of the Requirements, including any assumption that the Buyer or a third party will deliver any aspect of the Requirements or incur any cost related to the delivery of the Requirements

iv. ensure that pricing information is quoted in NZ$ exclusive of GST

v. if appropriate, obtain independent advice before submitting a Proposal

vi. satisfy itself as to the correctness and sufficiency of its Proposal, including the proposed pricing and the sustainability of the pricing.

d. There is no expectation or obligation for Respondents to submit Proposals in response to the RFP solely to remain on any prequalified or registered supplier list. Any Respondent on such a list will not be penalised for failure to submit a Proposal.

6.2 Offer Validity Period

a. Proposals are to remain valid and open for acceptance by the Buyer for the Offer Validity Period.

6.3 Respondents' Deadline for Questions

a. Each Respondent should satisfy itself as to the interpretation of the RFP. If there is any perceived ambiguity or uncertainty in the RFP document/s Respondents should seek clarification before the Deadline for Questions.

b. All requests for clarification must be made by email to the Buyer's Point of Contact. The Buyer will endeavour to respond to requests in a timely manner, but not later than the deadline for the Buyer to answer Respondents' questions in Section 1, paragraph 1.2.a, if applicable.

c. If the Buyer considers a request to be of sufficient importance to all Respondents it may provide details of the question and answer to other Respondents. In doing so the Buyer may summarise the Respondent's question and will not disclose the Respondent's identity. The question and answer may be posted on GETS and/or emailed to participating Respondents. A Respondent may withdraw a request at any time.

d. In submitting a request for clarification a Respondent is to indicate, in its request, any information that is commercially sensitive. The Buyer will not publish such commercially sensitive information. However, the Buyer may modify a request to eliminate such commercially sensitive information, and publish this and the answer where the Buyer considers it of general significance to all Respondents. In this case, however, the Respondent will be given an opportunity to withdraw the request or remove the commercially sensitive information.

6.4 Submitting a Proposal

a. Each Respondent is responsible for ensuring that its Proposal is received by the Buyer at the correct address on or before the Deadline for Proposals. The Buyer will acknowledge receipt of each Proposal.

b. The Buyer intends to rely on the Respondent's Proposal and all information provided by the Respondent (e.g. correspondence and negotiations). In submitting a Proposal and communicating with the Buyer each Respondent should check that all information it provides to the Buyer is:

   i. true, accurate and complete, and not misleading in any material respect

   ii. does not contain Intellectual Property that will breach a third party's rights.

c. Where the Buyer requires the Proposal to be delivered in hard and soft copies, the Respondent is responsible for ensuring that both the hard and soft copies are identical.

d. Where the Buyer stipulates a two envelope RFP process the following applies:

   i. each Respondent must ensure that all financial information and pricing components of its Proposal are provided separately from the remainder of its Proposal

   ii. financial information and pricing must be contained either in a separate sealed envelope or as a separate soft copy file (whichever option has be requested by the Buyer)

   iii. the pricing information must be clearly marked 'Financial and Pricing Information.' This is to ensure that the pricing information cannot be viewed when the package containing the other elements of the Proposal is opened.

Assessing Proposals

6.5 Evaluation panel

a. The Buyer will convene an evaluation panel comprising members chosen for their relevant expertise and experience. In addition, the Buyer may invite independent advisors to evaluate any Proposal, or any aspect of any Proposal.

6.6 Third party information

a. Each Respondent authorises the Buyer to collect additional information, except commercially sensitive pricing information, from any relevant third party (such as a referee or a previous or existing client) and to use that information as part of its evaluation of the Respondent's Proposal.

b. Each Respondent is to ensure that all referees listed in support of its Proposal agree to provide a reference.

c. To facilitate discussions between the Buyer and third parties each Respondent waives any confidentiality obligations that would otherwise apply to information held by a third party, with the exception of commercially sensitive pricing information.

6.7 Buyer's clarification

a. The Buyer may, at any time, request from any Respondent clarification of its Proposal as well as additional information about any aspect of its Proposal. The Buyer is not required to request the same clarification or information from each Respondent.

b. The Respondent must provide the clarification or additional information in the format requested. Respondents will endeavour to respond to requests in a timely manner. The Buyer may take such clarification or additional information into account in evaluating the Proposal.

c. Where a Respondent fails to respond adequately or within a reasonable time to a request for clarification or additional information, the Buyer may cease evaluating the Respondent's Proposal and may eliminate the Proposal from the RFP process.

6.8 Evaluation and shortlisting

a. The Buyer will base its initial evaluation on the Proposals submitted in response to the RFP. The Buyer may adjust its evaluation of a Proposal following consideration of any clarification or additional information as described in paragraphs 6.6 and 6.7.

b. In deciding which Respondent/s to shortlist the Buyer will take into account the results of the evaluations of each Proposal and the following additional information:

   i. each Respondent's understanding of the Requirements, capability to fully deliver the Requirements and willingness to meet the terms and conditions of the Proposed Contract

   ii. except where the price is the only criterion, the best value-for-money over the whole-of-life of the goods or services.

c. In deciding which Respondent/s, to shortlist the Buyer may take into account any of the following additional information:

   i. the results from reference checks, site visits, product testing and any other due diligence

   ii. the ease of contracting with a Respondent based on that Respondent's feedback on the Proposed Contract (where these do not form part of the weighted criteria)

   iii. any matter that materially impacts on the Buyer's trust and confidence in the Respondent

iv. any other relevant information that the Buyer may have in its possession.

d. The Buyer will advise Respondents if they have been shortlisted or not. Being shortlisted does not constitute acceptance by the Buyer of the Respondent's Proposal, or imply or create any obligation on the Buyer to enter into negotiations with, or award a Contract for delivery of the Requirements to any shortlisted Respondent/s. At this stage in the RFP process the Buyer will not make public the names of the shortlisted Respondents.

6.9 Negotiations

a. The Buyer may invite a Respondent to enter into negotiations with a view to contract. Where the outcome is unsatisfactory the Buyer may discontinue negotiations with a Respondent and may then initiate negotiations with another Respondent.

b. The Buyer may initiate concurrent negotiations with more than one Respondent. In concurrent negotiations the Buyer will treat each Respondent fairly, and:

i. prepare a negotiation plan for each negotiation

ii. advise each Respondent, that it wishes to negotiate with, that concurrent negotiations will be carried out

iii. hold separate negotiation meetings with each Respondent.

c. Each Respondent agrees that any legally binding contract entered into between the Successful Respondent and the Buyer will be essentially in the form set out in Section 5, the Proposed Contract.

6.10 Respondent's debrief

a. At any time after shortlisting Respondents the Buyer will offer all Respondents who have not been shortlisted a debrief. Each Respondent will have 30 Business Days, from the date of offer, to request a debrief. When a Respondent requests a debrief, the Buyer will provide the debrief within 30 Business Days of the date of the request, or of the date the Contract is signed, whichever is later.

b. The debrief may be provided by letter, email, phone or at a meeting. The debrief will:

i. provide the reasons why the Proposal was or was not successful

ii. explain how the Proposal performed against the pre-conditions (if applicable) and the evaluation criteria

iii. indicate the Proposal's relative strengths and weaknesses

iv. explain, in general terms, the relative advantage/s of the successful Proposal

v. seek to address any concerns or questions from the Respondent

vi. seek feedback from the Respondent on the RFP and the RFP process.

6.11 Notification of outcome

a. At any point after conclusion of negotiations, but no later than 30 Business Days after the date the Contract is signed, the Buyer will inform all unsuccessful Respondents of the name of the Successful Respondent, if any. The Buyer may make public the name of the Successful Respondent and any unsuccessful Respondent. Where applicable, the Buyer will publish a Contract Award Notice on GETS.

6.12 Issues and complaints

a. A Respondent may, in good faith, raise with the Buyer any issue or complaint about the RFP, or the RFP process at any time.

b. The Buyer will consider and respond promptly and impartially to the Respondent's issue or complaint.

c. Both the Buyer and Respondent agree to act in good faith and use their best endeavours to resolve any issue or complaint that may arise in relation to the RFP.
d. The fact that a Respondent has raised an issue or complaint is not to be used by the Buyer to unfairly prejudice the Respondent's ongoing participation in the RFP process or future contract opportunities.

Standard RFP conditions

6.13 Buyer's Point of Contact

a. All enquiries regarding the RFP must be directed by email to the Buyer's Point of Contact. Respondents must not directly or indirectly approach any representative of the Buyer, or any other person, to solicit information concerning any aspect of the RFP.

b. Only the Point of Contact, and any authorised person of the Buyer, are authorised to communicate with Respondents regarding any aspect of the RFP. The Buyer will not be bound by any statement made by any other person.
c. The Buyer may change the Point of Contact at any time. The Buyer will notify Respondents of any such change. This notification may be posted on GETS or sent by email.
d. Where a Respondent has an existing contract with the Buyer then business as usual communications, for the purpose of managing delivery of that contract, will continue using the usual contacts. Respondents must not use business as usual contacts to lobby the Buyer, solicit information or discuss aspects of the RFP.

6.14 Conflict of Interest

a. Each Respondent must complete the Conflict of Interest declaration in the Response Form and must immediately inform the Buyer should a Conflict of Interest arise during the RFP process. A material Conflict of Interest may result in the Respondent being disqualified from participating further in the RFP.

6.15 Ethics

a. Respondents must not attempt to influence or provide any form of personal inducement, reward or benefit to any representative of the Buyer in relation to the RFP.
b. A Respondent who attempts to do anything prohibited by paragraphs 6.13.a. and d. and 6.15.a. may be disqualified from participating further in the RFP process.
c. The Buyer reserves the right to require additional declarations, or other evidence from a Respondent, or any other person, throughout the RFP process to ensure probity of the RFP process.

6.16 Anti-collusion and bid rigging

a. Respondents must not engage in collusive, deceptive or improper conduct in the preparation of their Proposals or other submissions or in any discussions or negotiations with the Buyer. Such behaviour will result in the Respondent being disqualified from participating further in the RFP process. In submitting a Proposal the Respondent warrants that its Proposal has not been prepared in collusion with a Competitor.
b. The Buyer reserves the right, at its discretion, to report suspected collusive or anti-competitive conduct by Respondents to the appropriate authority and to give that authority all relevant information including a Respondent's Proposal.

6.17 Confidential Information

a. The Buyer and Respondent will each take reasonable steps to protect Confidential Information and, subject to paragraph 6.17.c. and without limiting any confidentiality

undertaking agreed between them, will not disclose Confidential Information to a third party without the other's prior written consent.

b. The Buyer and Respondent may each disclose Confidential Information to any person who is directly involved in the RFP process on its behalf, such as officers, employees, consultants, contractors, professional advisors, evaluation panel members, partners, principals or directors, but only for the purpose of participating in the RFP.

c. Respondents acknowledge that the Buyer's obligations under paragraph 6.17.a. are subject to requirements imposed by the Official Information Act 1982 (OIA), the Privacy Act 1993, parliamentary and constitutional convention and any other obligations imposed by law. The Buyer will not be in breach of its obligations if Confidential Information is disclosed by the Buyer to the appropriate authority because of suspected collusive or anti-competitive tendering behaviour. Where the Buyer receives an OIA request that relates to a Respondent's Confidential Information the Buyer will consult with the Respondent and may ask the Respondent to explain why the information is considered by the Respondent to be confidential or commercially sensitive.

6.18 Confidentiality of RFP information

a. For the duration of the RFP, to the date of the announcement of the Successful Respondent, or the end of the RFP process, the Respondent agrees to keep the RFP strictly confidential and not make any public statement to any third party in relation to any aspect of the RFP, the RFP process or the award of any Contract without the Buyer's prior written consent.

b. A Respondent may disclose RFP information to any person described in paragraph 6.17.b. but only for the purpose of participating in the RFP. The Respondent must take reasonable steps to ensure that such recipients do not disclose Confidential Information to any other person or use Confidential Information for any purpose other than responding to the RFP.

6.19 Costs of participating in the RFP process

a. Each Respondent will meet its own costs associated with the preparation and presentation of its Proposal and any negotiations.

6.20 Ownership of documents

a. The RFP and its contents remain the property of the Buyer. All Intellectual Property rights in the RFP remain the property of the Buyer or its licensors. The Buyer may request the immediate return or destruction of any or all RFP documents and any copies. Respondents must comply with any such request in a timely manner.

b. All documents forming the Proposal will, when delivered to the Buyer, become the property of the Buyer. Proposals will not be returned to Respondents at the end of the RFP process.

c. Ownership of Intellectual Property rights in the Proposal remain the property of the Respondent or its licensors. However, the Respondent grants to the Buyer a non-exclusive, non-transferable, perpetual licence to retain, use, copy and disclose information contained in the Proposal for any purpose related to the RFP process.

6.21 No binding legal relations

a. Neither the RFP, nor the RFP process, creates a process contract or any legal relationship between the Buyer and any Respondent, except in respect of:

   i. the Respondent's declaration in its Proposal

   ii. the Offer Validity Period

   iii. the Respondent's statements, representations and/or warranties in its Proposal and in its correspondence and negotiations with the Buyer

iv. the Evaluation Approach to be used by the Buyer to assess Proposals as set out in Section 3 and in the RFP-Terms (as varied by Section 1, paragraph 1.6, if applicable)

v. the standard RFP conditions set out in paragraphs 6.13 to 6.26

vi. any other matters expressly described as binding obligations in Section 1, paragraph 1.6.

b. Each exception in paragraph 6.21.a. is subject only to the Buyer's reserved rights in paragraph 6.23.

c. Except for the legal obligations set out in paragraph 6.21.a. no legal relationship is formed between the Buyer and any Respondent unless and until a Contract is entered into between those parties.

6.22 Elimination

a. The Buyer may exclude a Respondent from participating in the RFP if the Buyer has evidence of any of the following, and is considered by the Buyer to be material to the RFP:

i. the Respondent has failed to provide all information requested, or in the correct format, or materially breached a term or condition of the RFP

ii. the Proposal contains a material error, omission or inaccuracy

iii. the Respondent is in bankruptcy, receivership or liquidation

iv. the Respondent has made a false declaration

v. there is a serious performance issue in a historic or current contract delivered by the Respondent

vi. the Respondent has been convicted of a serious crime or offence

vii. there is professional misconduct or an act or omission on the part of the Respondent which adversely reflects on the integrity of the Respondent

viii. the Respondent has failed to pay taxes, duties or other levies

ix. the Respondent represents a threat to national security or the confidentiality of sensitive government information

x. the Respondent is a person or organisation designated as a terrorist by New Zealand Police.

6.23 Buyer's additional rights

a. Despite any other provision in the RFP the Buyer may, on giving due notice to Respondents:

i. amend, suspend, cancel and/or re-issue the RFP, or any part of the RFP

ii. make any material change to the RFP (including any change to the timeline, Requirements or Evaluation Approach) on the condition that Respondents are given a reasonable time within which to respond to the change.

b. Despite any other provision in the RFP the Buyer may:

i. accept a late Proposal if it is the Buyer's fault that it is received late

ii. in exceptional circumstances, accept a late Proposal where it considers that there is no material prejudice to other Respondents. The Buyer will not accept a late Proposal if it considers that there is risk of collusion on the part of a Respondent, or the Respondent may have knowledge of the content of any other Proposal

iii. in exceptional circumstances, answer a question submitted after the Deadline for Questions, if applicable

iv. accept or reject any Proposal, or part of a Proposal

v. accept or reject any non-compliant, non-conforming or alternative Proposal

vi. decide not to accept the lowest priced conforming Proposal unless this is stated as the Evaluation Approach

vii. decide not to enter into a Contract with any Respondent

viii. liaise or negotiate with any Respondent without disclosing this to, or doing the same with, any other Respondent

ix. provide or withhold from any Respondent information in relation to any question arising in relation to the RFP. Information will usually only be withheld if it is deemed unnecessary, is commercially sensitive to a Respondent, is inappropriate to supply at the time of the request or cannot be released for legal reasons

x. amend the Proposed Contract at any time, including during negotiations with a shortlisted Respondent

xi. waive irregularities or requirements in or during the RFP process where it considers it appropriate and reasonable to do so.

c. The Buyer may request that a Respondent/s agrees to the Buyer:

i. selecting any individual element/s of the Requirements that is offered in a Proposal and capable of being delivered separately, unless the Proposal specifically states that the Proposal, or elements of the Proposal, are to be taken collectively

ii. selecting two or more Respondents to deliver the Requirements as a joint venture or consortium.

6.24 New Zealand law

a. The laws of New Zealand shall govern the RFP and each Respondent agrees to submit to the exclusive jurisdiction of the New Zealand courts in respect of any dispute concerning the RFP or the RFP process.

6.25 Disclaimer

a. The Buyer will not be liable in contract, tort, equity, or in any other way whatsoever for any direct or indirect damage, loss or cost incurred by any Respondent or any other person in respect of the RFP process.

b. Nothing contained or implied in the RFP, or RFP process, or any other communication by the Buyer to any Respondent shall be construed as legal, financial or other advice. The Buyer has endeavoured to ensure the integrity of such information. However, it has not been independently verified and may not be updated.

c. To the extent that liability cannot be excluded, the maximum aggregate liability of the Buyer, its agents and advisors is $1.

6.26 Precedence

a. Any conflict or inconsistency in the RFP shall be resolved by giving precedence in the following descending order:

i. Section 1, paragraph 1.6

ii. Section 6 (RFP-Terms)

iii. all other Sections of this RFP document

iv. any additional information or document provided by the Buyer to Respondents through the Buyer's Point of Contact or GETS.

b. If there is any conflict or inconsistency between information or documents having the same level of precedence the later information or document will prevail.

Definitions

In relation to the RFP the following words and expressions have the meanings described below.

Advance Notice	A notice published by the buyer on GETS in advance of publishing the RFP. An Advance Notice alerts the market to a contract opportunity. Where used, an Advance Notice forms part of the RFP.
Business Day	Any week day in New Zealand, excluding Saturdays, Sundays, New Zealand (national) public holidays and all days from Boxing Day up to and including the day after New Year's Day.
Buyer	The Buyer is the government agency that has issued the RFP with the intent of purchasing the goods or services described in the Requirements. The term Buyer includes its officers, employees, contractors, consultants, agents and representatives.
Competitors	Any other business that is in competition with a Respondent either in relation to the goods or services sought under the RFP or in general.
Confidential Information	Information that: a. is by its nature confidential b. is marked by either the Buyer or a Respondent as 'confidential', 'commercially sensitive', 'sensitive', 'in confidence', 'top secret', 'secret', classified' and/or 'restricted' c. is provided by the Buyer, a Respondent, or a third party in confidence d. the Buyer or a Respondent knows, or ought to know, is confidential. Confidential information does not cover information that is in the public domain through no fault of either the Buyer or a Respondent.
Conflict of Interest	A Conflict of Interest arises if a Respondent's personal or business interests or obligations do, could, or be perceived to, conflict with its obligations to the Buyer under the RFP or in the provision of the goods or services. It means that the Respondent's independence, objectivity or impartiality can be called into question. A Conflict of Interest may be: a. actual: where the conflict currently exists b. potential: where the conflict is about to happen or could happen, or c. perceived: where other people may reasonably think that a person is compromised.
Contract	The written Contract/s entered into by the Buyer and Successful Respondent/s for the delivery of the Requirements.
Contract Award Notice	Government Rules of Sourcing, Rule 45 requires a Buyer to publish a Contract Award Notice on GETS when it has awarded a contract that is subject to the Rules.
Deadline for Proposals	The deadline that Proposals are to be delivered or submitted to the Buyer as stated in Section 1, paragraph 1.2.
Deadline for Questions	The deadline for suppliers to submit questions to the Buyer as stated in Section 1, paragraph 1.2, if applicable.
Evaluation Approach	The approach used by the Buyer to evaluate Proposals as described in Section 3 and in Section 6 (as varied by Section 1, paragraph 1.6, if applicable).
GETS	Government Electronic Tenders Service available at www.gets.govt.nz

GST	The goods and services tax payable in accordance with the New Zealand Goods and Services Tax Act 1985.
Intellectual Property	All intellectual property rights and interests, including copyright, trademarks, designs, patents and other proprietary rights, recognised or protected by law.
Offer Validity Period	The period of time when a Proposal (offer) is held open by the Respondent for acceptance by the Buyer as stated in Section 1, paragraph 1.6.
Point of Contact	The Buyer and each Respondent are required to appoint a Point of Contact. This is the channel to be used for all communications during the RFP process. The Buyer's Point of Contact is identified in Section 1, paragraph 1.3. The Respondent's Point of Contact is identified in its Proposal.
Price	The total amount, including all costs, fees, expenses and charges, to be charged by the Successful Respondent for the full delivery of the Requirements. Each Respondent's Proposal must include its Price.
Proposal	The response a Respondent submits in reply to the RFP. It comprises the Response Form, the Respondent's bid, financial and pricing information and all other information submitted by a Respondent.
Proposed Contract	The Contract terms and conditions proposed by the Buyer for the delivery of the Requirements as described in Section 5.
RFP	Means the Request for Proposal.
Registration of Interest	A formal request by a Buyer asking potential suppliers to register their interest in a procurement. It is the first step in a multi-step tender process.
Request for Proposal (RFP)	The RFP comprises the Advance Notice (where used), the Registration of Interest (where used), this RFP document (including the RFP-Terms) and any other schedule, appendix or document attached to this RFP, and any subsequent information provided by the Buyer to Respondents through the Buyer's Point of Contact or GETS.
RFP-Terms	Means the Request for Proposal - Process, Terms and Conditions as described in Section 6.
RFP Process, Terms and Conditions (shortened to RFP-Terms)	The government's standard process, terms and conditions that apply to RFPs as described in Section 6. These may be varied at the time of the release of the RFP by the Buyer in Section 1, paragraph 1.6. These may be varied subsequent to the release of the RFP by the Buyer on giving notice to Respondents.
Requirements	The goods and/or services described in Section 2 which the Buyer intends to purchase.
Respondent	A person, organisation, business or other entity that submits a Proposal in response to the RFP. The term Respondent includes its officers, employees, contractors, consultants, agents and representatives. The term Respondent differs from a supplier, which is any other business in the market place that does not submit a Proposal.
Response Form	The form and declaration prescribed by the Buyer and used by a Respondent to respond to the RFP, duly completed and submitted by a Respondent as part of the Proposal.
Successful Respondent	Following the evaluation of Proposals and successful negotiations, the Respondent/s who is awarded a Contract/s to deliver all or part of the Requirements.

ABIS 2 Detailed Requirements Document

Glossary of Terms

Glossary of terms used within or abbreviations used within this document.

Term	Description
ABIS	Automated Biometric Information System
Charge Group	Managed by NIA, the Charge Group contains charges laid as the result of an incident or arrest. Biometric data is managed against a group of charges rather than each individual charge.
Firearms Licence Holder	Person who has provided details, including photograph as part of an application for a Firearms Licence or renewal of an existing Firearms Licence. A person may have two separate Firearms Licences, one as an individual and one as a dealer. • Generate a file for new and renewed Firearms Licence details and an associated image for production of Firearms Licences (by an external supplier).
Formal Photo	Image(s) obtained pursuant to legislation related to an arrest, charge, summons, returned offenders or CPOR managed individuals. In some current state documentation this may be referred to as a Prisoner photo.
Image Management Functions/Features	Those features that the application uses to : • Import and storage of facial images captured within multiple business processes • Import, classify and storage of SMT and clothing images captured within multiple business processes • Management of stored facial, SMT and clothing image • Interface to NZ Police's operational applications (including but not limited to National Intelligence Application (NIA)) for retrieval of personal attributes related to an image. Search and retrieve facial and SMT images using text based attribute searching. • Meet American National Standards Institute / National Institute of Standards and Technology (ANSI/NIST) minimum standard.
IMS	Image Management System

Line-Up / Photo Line-Up	A group of images displayed to allow a witness to identify a suspect. This is not a line of people for the witness to view. In some jurisdictions this is known as a Montage.
Livescan	Solution for the electronic capture of biometric information (fingerprints and photo graphs) by frontline staff.
Missing Person	An individual who has been reported as missing and the subject of Missing Person processes. An individual who is the subject of Disaster Victim Identification (DVI) process.
Noting ID	Managed by NIA, unique reference to a given event that resulted in on or more incidents/offences and subsequent charges Also known as Occurrence ID or Record ID.
NRS	National Recording Standard. Defines the information to be collected by NZP for specific business scenarios.
NZP operational	The group of applications NZP use to support the day to day policing operational needs. These applications sit outside the scope of this solution but will interact with the proposed solution.
NZP operational data set	NZP use multiple integrated applications and products to support day to day policing operational needs. The high level of integration requires a common definition of attributes and terminology across the different components. The NZP operational data set provides a common definition for shared attribution.
Offender	Offender or alleged offender has had biometric details (eg fingerprint, photographs) captured under the provision of Section 32 or 33 of the Policing Act. Person who is/or will be charged with an offence. May or may not be taken into custody. Sometimes referred to as Prisoner, this term is used within the existing Image Management system (IMS).
Person Dossier ID	Managed by NIA, the Person dossier ID is the unique key for a Person.
Photo Books and Photo Line Up functions	Those features that the application uses to : • Enable the production of Photo Books to allow the classification of photos by type. • Enable the provision for evidential purposes a mechanism to produce Formal Photo Line-ups using Formal Photos. This will include the capability to interface with NZ Police operational application (OnDuty)

	which would manage the mobile user's need within a single integrated application. The objective being police being able to show a witness a series of photographs on their mobility device in the future.
Photo Manager	Desktop software of the existing Image Management System.
Photo Recognition functions/features	Those features that the application uses to : • Enable the use of advance suspect or victim identification using facial recognition.
SMT	Scars, Marks and Tattoos for an individual. Also known as Body Marks.
SMT Recognition functions/features	Those features that the application uses to : • Enable the use of advance suspect or victim identification using facial recognition, SMT and clothing symbol/pattern recognition.
Suspect	An individual believed to be involved in an incident or offence.
TCN	Transaction Control Number. Unique key given to a set of fingerprints and photos captured by Livescan or ABIS.
Voluntary	Image(s) of an individual that have been provided to voluntary provided to Police.

1 Current State

1.1 History

The existing image management system (Photo Manager) was fully implemented by Police in 2009 to replace the Photographic Image Management System (PIMS) which was a standalone system implemented by Police in 1992. Photo Manager has provided a single repository for all identification images including Formal Prisoner Photographs, Firearms Licence holders, Suspect images and Missing Persons images but has limited facial recognition capability.

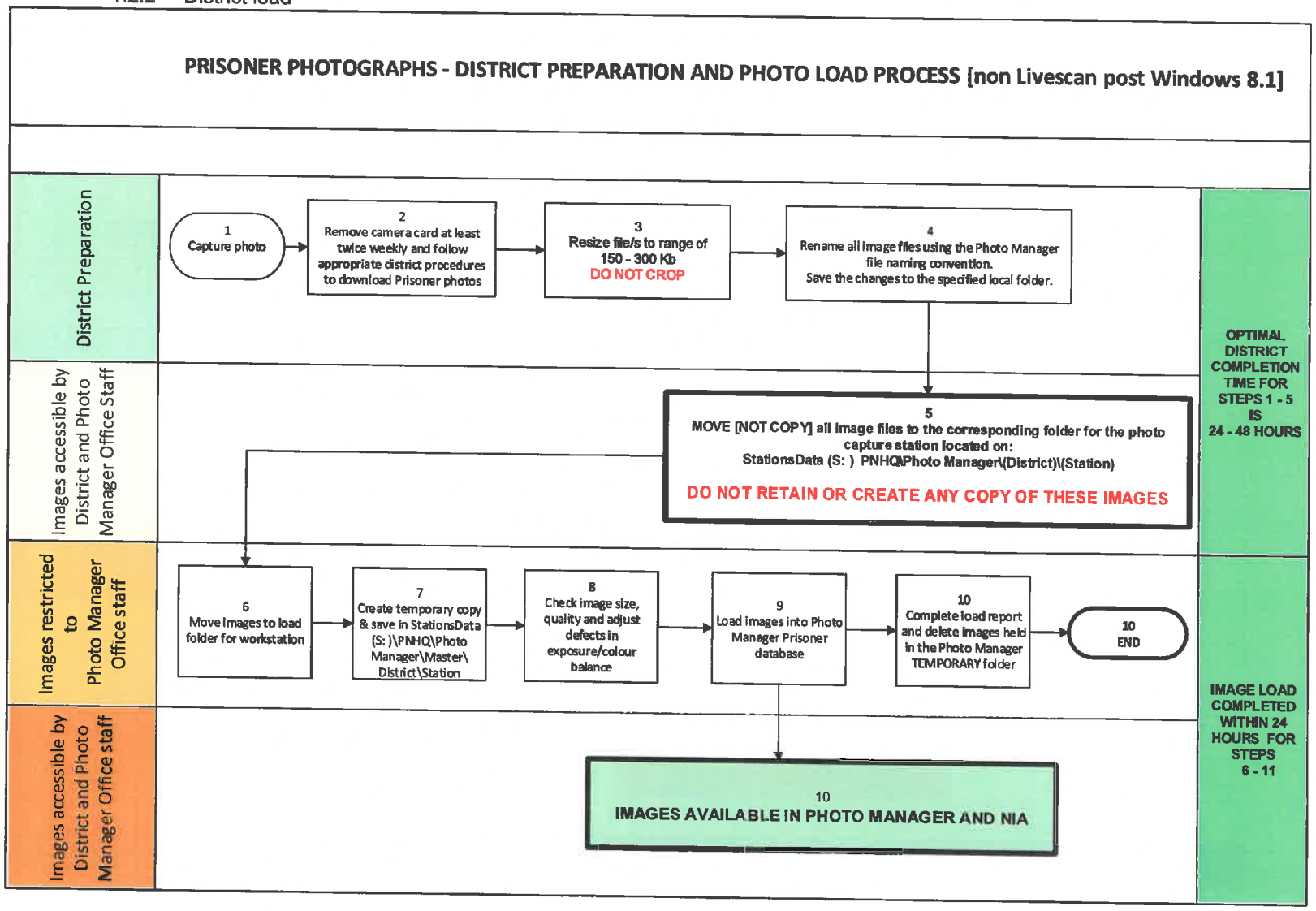
Currently scars, marks and tattoo details are held in a coded/text format and the current clothing description database is held in a spreadsheet format. There are currently no image based capabilities able to capture, classify and search soft biometrics; scars, marks and tattoos for biometric identification or classify and search clothing images for intelligence.

1.2 Business Process

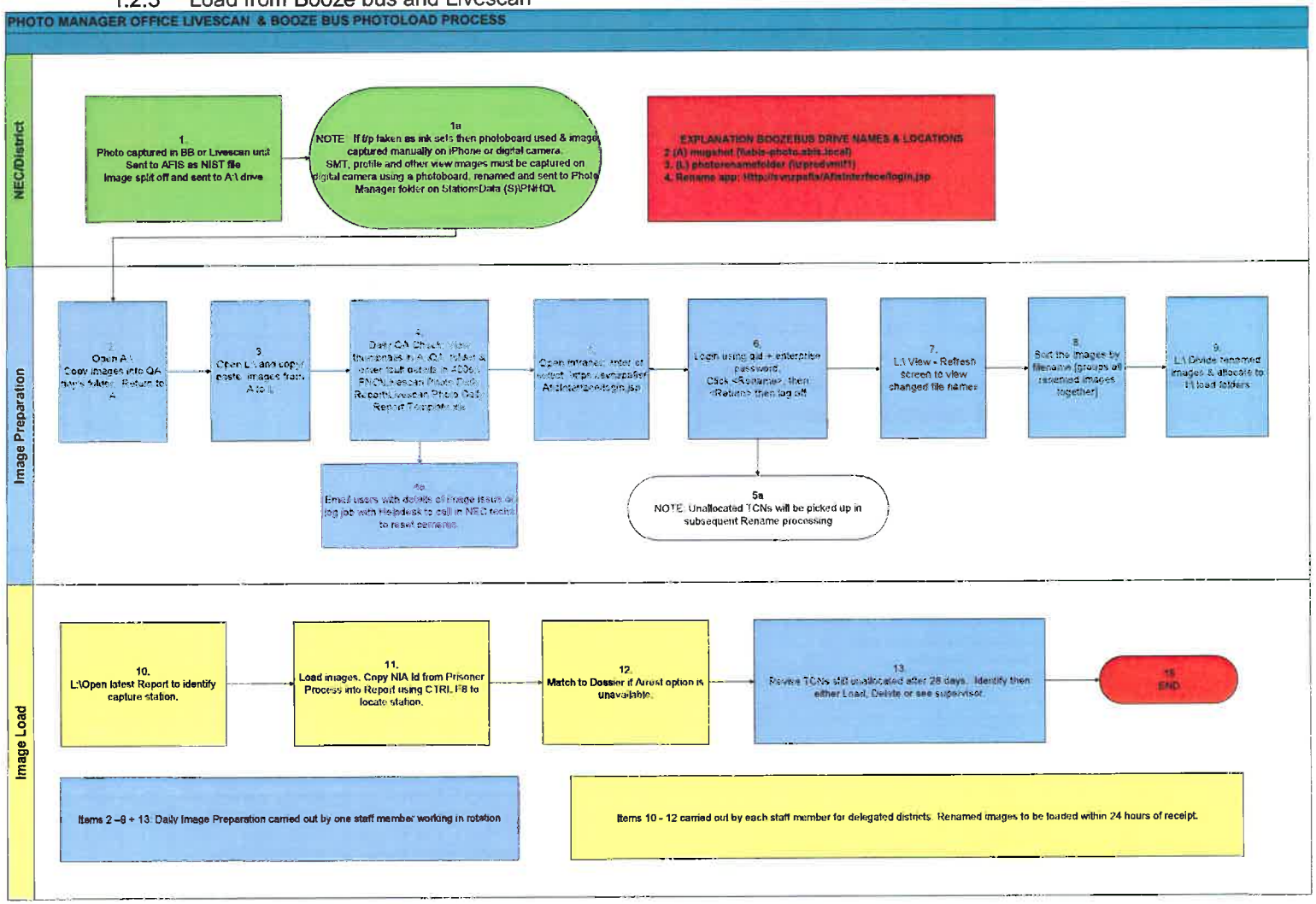
1.2.1 Firearms Licence batch process.

Batching occurs every Monday morning before 10am where the IMS card data is extracted from NIA and then digitally sent to ABCorp, the card manufacturers. This process involves a 2-step process and then emailing the card manufacturers, ABCorp/firearms licencing administrators that it has been completed. During the batching, it is advised that there is no processing of datasheets until the data is sent to avoid complications.

1.2.2 District load



1.2.3 Load from Booze bus and Livescan



1.3 System Overview

1.3.1 Image repositories

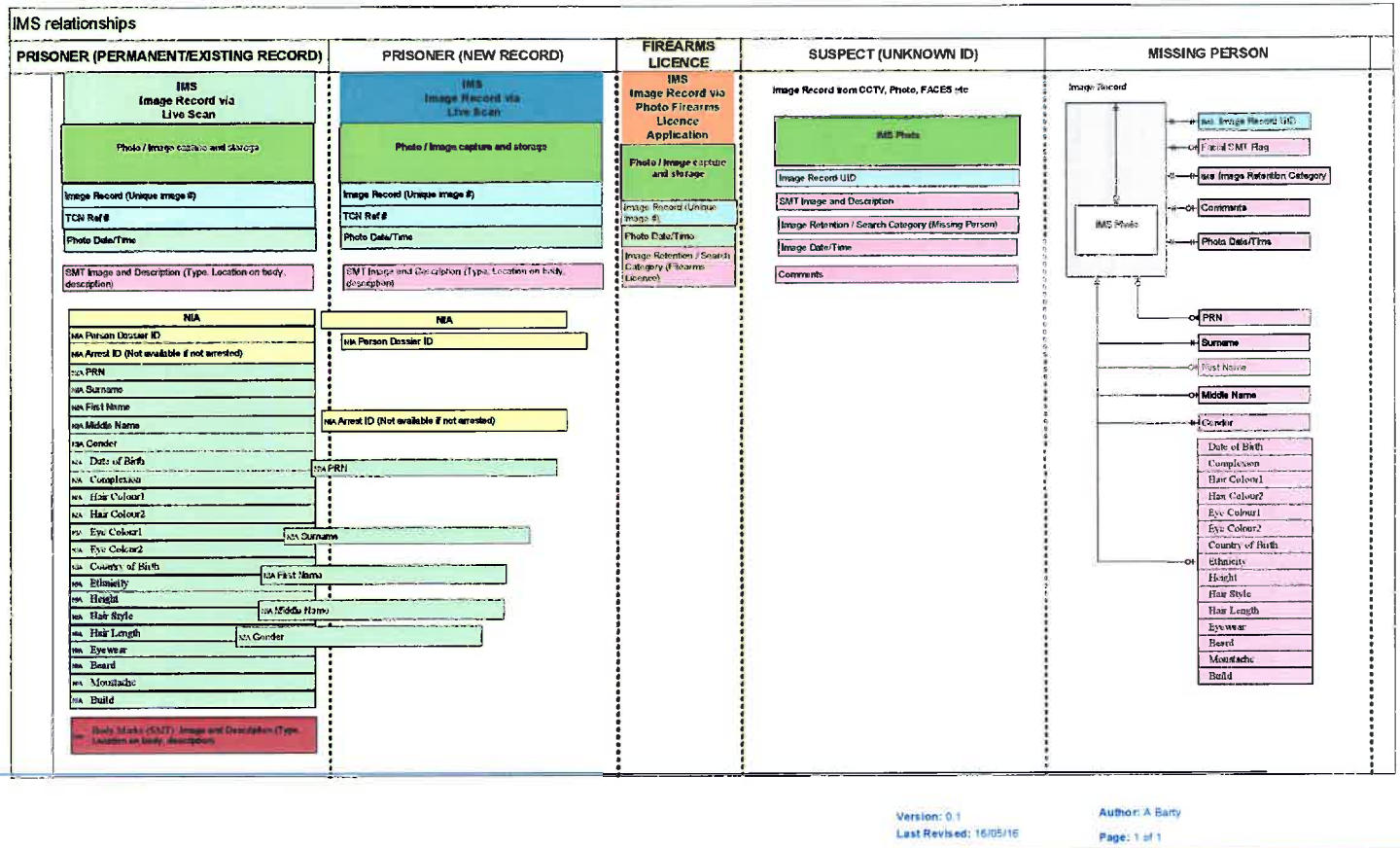
Repository	Contains		
Formal Photos	Offender	• Arrested	Section 32 &33 Policing Act.
		• Charged	Section 32 &33 Policing Act.
		• Summons	Section 32 &33 Policing Act.
	CPOR		
	Returned Offenders		Photographed on return to NZ. Cannot be used as Photo Line Up filler image.
Voluntary		• Youth • On request	
Firearms Licence			
Suspect			
Missing Person			
Deceased			Note 2

Notes:

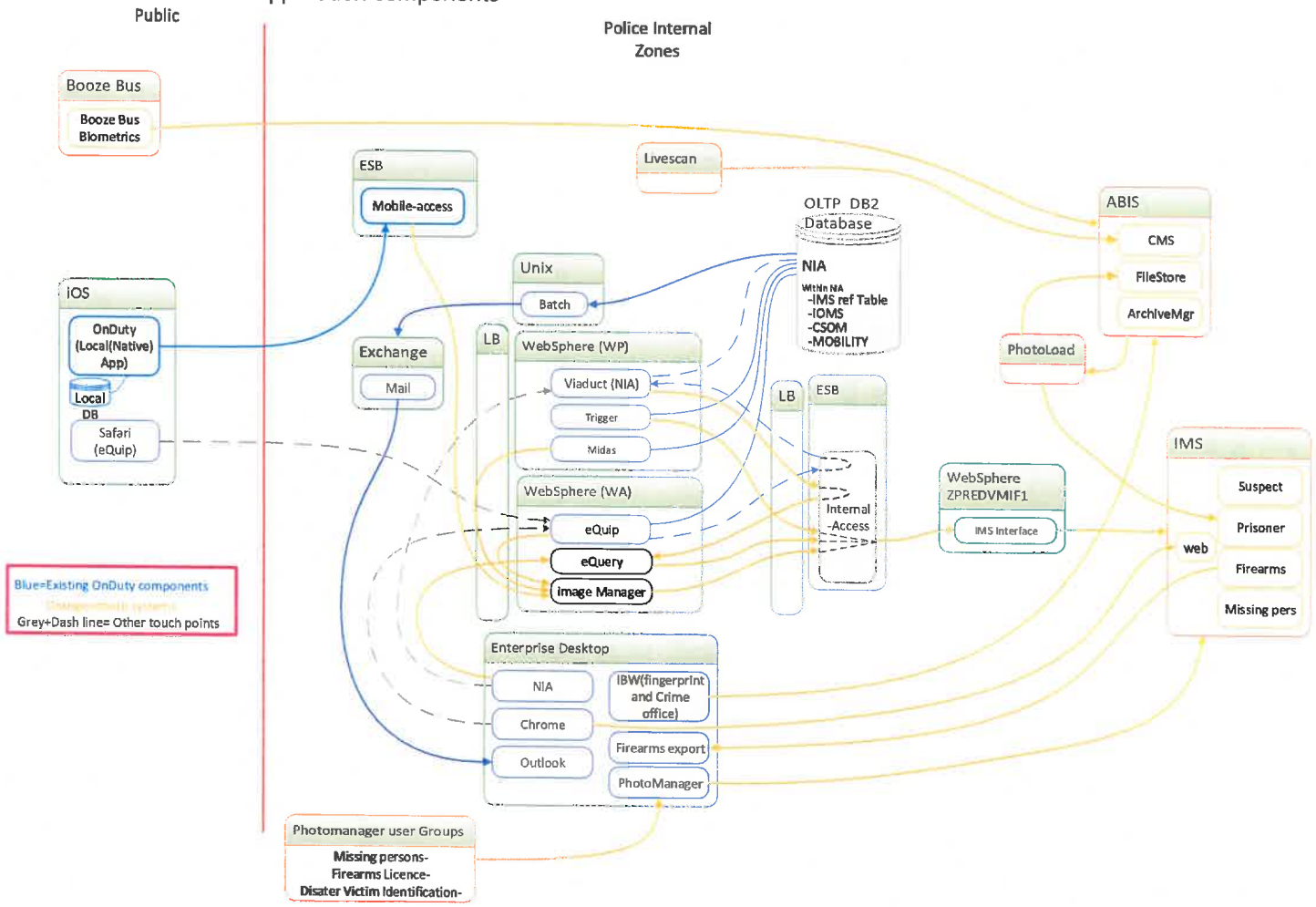
1. Images held within IMS are migrated to a separate repository when the National Biometrics Office is advised of the death. Within the new system the identity can remove within the original repository and be flagged as deceased. Deceased person may be included within recognition searching but must be excluded from use as Photo Line Up filler images.

1.3.2 Conceptual model

Conceptual facial recognition (capture / SMT classification / storage / comparison relationship model - Image Management System and NIA



1.3.3 Infrastructure and application components



ESB (Internal DataPower)

Existing police infrastructure, IBM DataPower XML firewall devices with Enterprise Service Bus capability. An XML firewall is a specialized firewall used to provide security for XML messaging such as Web services (communication between computer systems).

The Internal DataPower is on the ECN and is providing two way TLS and message signing for secure communication, translation and validation services where required for middleware and other services e.g. any third party systems Web services on the ECN.

- Mobile-Access

  A core component for the OnDuty architecture, is a dedicated routing connector domain (mostly REST) in the ESB for mobile devices. This provides a single landing point for OnDuty in the ESB, the ESB can then interpret the packages and direct them to the correct services as required. In this case packages are routed to the Image Manager application.

- Internal-Access

  A routing connector domain (mostly SOAP) in the ESB. Like "Mobile-Access", but for all other systems. ESB can then interpret the packages and direct them to the correct services as required. In this case there are many different traffic routings, NIA connects to eQuip and eQuery via Internal access and trigger, eQuery and Image Manager all go through Internal Access to the IMS interface.

Middleware - WebSphere (WP)

WebSphere Application Server Processing (WP) cell. A group/cluster (cell) of WebSphere Application Servers where Police deploy stateless Java Processing Applications. These are back end applications with no end user browser style connectivity.

The following applications are delivered on the WP:

- Viaduct(NIA)

  An existing Police application in WebSphere WP that is the processing engine for the NIA database and the back end to the NIA client. Viaduct is used for specific calls to the NIA database.

- Trigger Process

  For CVIR the Trigger Process will manage the processing of completed IONS and WTW by Midas, as and when Midas resources are available.

  For TCR trigger will pick up a flag that a TCR is completed and process that TCR through to NZTA

- Midas

  This is a Java application deployed to WebSphere WP to handle all Mobility services (SMART and any future apps) that the iOS devices will need to use. It will use Jersey as an engine for managing RESTful services that map onto either current ESB services or to interact directly with services provided in the Mobility Services layer.

  Midas will request image data through Image Manager.

Middleware - WebSphere (WA)

WebSphere Application Server (WA) cell. A group/cluster (cell) of WebSphere Application Servers where Police deploy state full Java Web Applications. These are back end applications that are visible to users as they host an end user browser style connectivity.

The following applications are delivered by the WA:

- eQuip

  eQuip is an existing internally developed web application that has been made available for access using the web browser on all Police devices. It is designed for mobile use on both iPhone and iPad using Safari, as well as the enterprise desktop using Chrome. eQuip is built using the Wicket framework developed by Apache and is a Web based platform for simplified NIA type actions. The OnDuty application will gradually replace the mobile use of eQuip, but desktop eQuip will still be used for station based queries and processing of TCR's.

  eQuip will request image data through Image Manager.

- eQuery

  eQuery is also an existing internally developed web application that has been made available for access using the web browser on all Police devices. It is designed for web based access and presentation of NIA data.

  eQuery will go to the ESB Internal Access connector to request image data from the IMS Interface.

- Image Manager

  Image Manager is a NZP developed application that interfaces with IMS to provide a shared set of services for OnDuty, Midas and eQuery. It also has a cache for photos with a TTL of 5mins to buffer the rapid repeat calls from our OnDuty application.

ZDREDVMIF1

WebSphere Interface Server (IF). A single server where Police deploy stateless Java Web Applications that are interfacing systems. This server has no clustering. These are back end applications with no end user browser style connectivity.

- IMS Interface

  IMS Interface is also an existing internally developed web application to enable fast, easy connections to IMS to receive photos for NIA and Mobility. Initially for NIA only it is also known as IMS NIA Interface.

OLT DB2 Database

- NIA

Existing Police NIA database hosted on a DB2 database server cluster. The NIA database hosts the Mobility and SMART schemas. Viaduct is the processing engine for the Nia Database and any data processed on the mobile device, or by the middleware, that is to be transferred into NIA should first be quality validated, e.g. by a workflow process.

- Mobility

The Mobility database is an existing database with a separate schema within the NIA DB2 database. Mobility DB was originally used by eQuip and the common services contained within eQuip will be separated out into a new layer called Mobility Services. These services manage the local storage of data in the Mobility schema. Both eQuip and Midas will use these services thereby ensuring a common implementation between the iOS devices using Midas and other devices using eQuip.

- IOMS (Corrections)

IOMS is a separate schema in NIA with a nightly data upload from Corrections

NZP access to images is through eQuery (there is a link in the NIA App that opens eQuery as if it is part of NIA)

It has all prisoner info except photos, if the prisoner is on the CPOR list it will include their photo as well.

- CSOM

CSOM is a special schema that may contain photos

- IMS reference tables

There are a set of IMS reference tables in NIA for quick reference of types of records held in IMS for NIA identities.

Enterprise Desktop

The enterprise desktop is user devices running Windows OS and include laptops and tablets.

- Chrome Browser (eQuip and WEB Photomanager)

  Chrome is the preferred browser for use to access the WEB interface of eQuip. It can also be used to access the WEB interface of Photomanager, the IMS application. Web Photomanager has less functionality then the full workstation client so is just there for easy view access to the IMS system, The enterprise desktop will provide a faster and richer interface to eQuip, with more viewing real-estate than available on the mobile device. eQuip is mostly used by the File Management Centre (FMC) for quality management of data going to NIA.

- NIA Application

  The NIA application is an internally developed application and available on all police Windows devices. This provides access to the NIA DB through Viaduct. It also interfaces with eQuery to access photos from IMS

- Photo Manager(client for IMS)

  Photo Manager client is installed on ~50 std police workstations around the country. It is used to administer maintain the Photomanager system and for firearms licence processing, missing persons and offender photo line-ups etc.

- IBW(client for ABIS)

  The workstation application for ABIS (IBW) is installed on ~26 std police workstations. The numbers are limited as the licence is expensive. The workstations are used by the fingerprints and crime offices and will also include a scanner and/or camera for recording images of prints from evidence etc. The installation of IBW on the workstation has to be done for each user using the application as there is a per user install component

- Firearms Export

  By DataWorks Plus, the NZ Firearms Licence Export application is a small manually installed application solely for extracting information from IMS to pass onto a vendor for printing of firearms licences. It is only installed on up to five workstations in the firearms processing team offices.

- Outlook

  Outlook is the Mail client installed on all NZP desktops, It will receive the email sent by the batch process to the Microsoft Exchange Mail servers. The email is the list of photos that need to be destroyed.

OnDuty iPhone and OnDuty Native iOS Application

The OnDuty iOS client application is made up of two components the iOS app and local application databases (Local DB):\

- iOS (Local (Native) App)

  OnDuty mobile application is a joint development between Police and Smudge, this application forms the framework for future functionality/capabilities required to enable frontline officers to manage/perform their policing activities and taskings.

  The OnDuty mobile client application will have the facility to share data between multiple iOS devices belonging to the same user, and also between devices belonging to other users in the same unit.

  The application pulls photos/thumbnails as required for viewing directly from the Image Manager, whereas all other data is received from Midas.

- Local DB

  Within the OnDuty application there will be a number of local relational databases implemented, with the following characteristics:

  - Will synchronise data from and to the enterprise on a regular basis.
  - Provide all necessary reference and application lookup data to allow the application to work offline.
  - Each database will have the appropriate security in line with the level of sensitivity of the data.
  - Provide the capability to store User data entry information in an offline state and synchronise this data entry information.

- Safari Browser (eQuip)

  eQuip is an existing internally developed web application that has been made available for access using the Safari web browser on Police iOS devices. It is designed for mobile use on both iPhone and iPad, as well as the enterprise desktop. The OnDuty application will gradually replace the mobile use of eQuip, but desktop eQuip will still be used for station based queries and processing of TCR's.

LB (WebSphere – Load Balancer)

Existing Police load balancing service predominantly and extensively used to front WebSphere applications and the ESB, but is also available to other systems where they do not have their own load balancing service.

ABIS (Automated Biometric Identification System)

Internally hosted, but external party managed (on site, no external connection), ABIS is mostly for Fingerprints, but does capture Facial photos for transfer, using Photo load, into IMS where they are stored and managed for use.

There are also 50 Livescan stations and 21 Booze buses laptops where they can process fingerprints and facial photos during an arrest.

ABIS uses Transaction Number (TCN) as key for all the scan event data.

Scan event images are deleted if the charge is dropped, but some other scan event metadata is retained.

There are two main NIA interfaces, during charge processing ABIS gets person of interest alert (just an alert, it has no details) from NIA. At the end of processing sends TCN and ABIS numbers and a combined TCN+ABIS number string is sent to NIA.

Livescan

The LiveScan terminal is a dedicated device for collecting fingerprints and facial photos for ABIS. It is a NZP custom windows 7 build with the Livescan software and device drivers for fingerprint scanner and camera. The PC is locked in a cabinet for security, there are roughly 50 units distributed around the country.

Booze Bus

The Booze Bus terminal is a dedicated Laptop for collecting fingerprints and facial photos for ABIS while mobile in a specialist van for roadside processing of drunk drivers (Booze Bus). It is a NZP custom windows 7 build with custom software Booze Bus Biometrics (BBB) and device drivers for CrossMatch fingerprint scanner and camera. The laptop is mobile and can be removed from the specialist van, there are roughly 21 BBB laptops.

PhotoLoad

PhotoLoad is a back end application used to transfer photos from ABIS to IMS and associate the photo with a person in NIA. The process includes the "Crossmatch Image Renaming Utility" and renames the file to the IMS format and saves copies to a file share on the ABIS sever infrastructure under PhotoRename/Reports/ and Backup/*station name*/.

IMS(Photo Store)

The Image Management System (IMS) is by Photomanager and is the back end that provides the system for storing and processing photos and associated metadata.

Suspect, Prisoner, Firearms and Missing persons are the four separate databases of images within IMS.

Web is a web interface to the IMS with restricted level of functionality.

Missing persons DB has is no electronic link to NIA and is accessed directly on IMS using the PhotoManager application from a NZP workstation

The person in NIA is linked to the photo in IMS by the IMS number in NIA and NIA ID in IMS.

NIA has separate link to each photo type, Firearms and Charge (clearly identifies the source of photo).

OnDuty does not differentiate between the photo sources and just provides the latest one.

1.3.4 ICT operational environment

I. NZ Police consume a whole of government 'Desktop as a Service' provisioned by Spark. Currently Windows 8.1, moving to Windows 10.
II. NZ Police consume email (largely) as a service, also provisioned by Spark. Currently MS Exchange 2013, with Outlook clients from Office 2013.
III. NZ Police consume Backup as a Service, provisioned by Revera/Spark. Currently ComVault v11.

IV. NZ Police consume 'Mobility' as a service, provisioned on Apple iOS devices managed by AirWatch (MDM) by Vodafone.
V. NZ Police consume Data Centre resource, provisioned as 'Colo' (hosting) by Revera – across multiple data centres.
VI. NZ Police operate ArcSight as our SIEM solution.
VII. NZ Police operate Symantec Enterprise Vault as our email archiving solution.
VIII. NZ Police operate our own 24/7 Help Desk, using HEAT (application) as our primary management tool.
IX. NZ Police operate an 'in house' Application support team.
X. NZ Police operate an 'in house' DBA team.
XI. NZ Police operate an 'in house' Firewall administration team.
XII. NZ Police operate an 'in house' telephony / voice administration team.
XIII. NZ Police operate an 'in house' network support team.
XIV. NZ Police operate 'in house' server (VMware/Windows/Linux) support teams.
XV. NZ Police operate IBM DataPower devices providing ESB/SOA services.
XVI. NZ Police operate IBM WebSphere application and integration middleware.
XVII. NZ Police operate IBM WebSphere edge servers as Load Balancers.
XVIII. NZ Police operate IBM DB2, Oracle and MS SQL servers.
XIX. NZ Police operate VMWARE (virtual server) Hypervisors.
XX. NZ Police operate MS Active directory servers.
XXI. NZ Police operate Windows servers.
XXII. NZ Police operate RHEL servers.
XXIII. NZ Police operate a nationwide radio network.
XXIV. NZ Police operate 3 24/7 emergency (111) call centres.
XXV. NZ Police operate ITM (IBM Tivoli Monitoring) on Linux (RHEL) servers.
XXVI. NZ Police operate OpManager monitoring on Windows servers.
XXVII. NZ Police operate an internal AD integrated PKI infrastructure. NZ Police expect all internal websites will use SSL/TLS and make certificates available to ensure this.
XXVIII. NZ Police operate a (BlueCoat) proxy server controlling internet access. Direct access to the internet is not permitted. Internet access is restricted by user account, with a small number of exceptions made for specific host servers (fetching of patches, AV updates etc.).
XXIX. NZ Police operate 'CheckPoint' media encryption software, ensuring all data written to portable media is encrypted.
XXX. NZ Police operate 'Secure Print' printing, ensuring that users identify themselves to a printer before printing takes place.
XXXI. NZ Police operate eGuardPost for remote vendor access (TPAM). Access is recorded, and management approved for each occasion. Suitable only for short term system access, for fault finding or system repair. Alternative remote access solutions considered on a case by case basis.

1.3.5 NZ Police Network Environment

I. NZ Police operate a private, internal IP (Internet Protocol) network, with no (physical or firewall) separation between test and production environments. The network carries internal voice traffic (VOIP).
II. Solution QOS requirements must be defined and approved.
III. Solutions requiring network services between WPD, ART and Communications Centres (Auckland, Wellington, Christchurch 111 call centres) should run with a network response time of up to 100msec RTT.
IV. Solutions must not transmit files larger than 1GB across the wide area network including Wi-Fi without network approval.
V. Solutions should operate within a 160 millisecond, or less, client to server round-trip and with a minimum of 0.5% packet loss for voice/real-time traffic.
VI. Solutions with users who are within National Headquarters, the major district centres, or the ICT service centre, the solution should run over a maximum 20Mb link.
VII. Solutions with users who can be anywhere on the Police network including WAN, LAN, Satellite, Mobile and Wi-Fi, should run with a network response time up to 1000ms RTT.
VIII. Solutions with users who can be anywhere on the Police network, applications should run over a 1024Kb or greater link.
IX. Use of Jumbo Frames is by negotiation with ICT Network Management.

1.3.6 Interfaces to NZP core applications (excluding ABIS).
Existing interfaces between Police applications and the Image Manager System (Photo Manager) support the loading, use and identity management for facial photos. Unique keys and meta-data are currently shared across the integrated applications to support the system to system interfacing.

Look up Person details for a formal photo.	Purpose:	IMS to request person details for a known individual/charge as part of the Image Load process. Successful completion of this transaction will result in an update of Image metadata within NIA for the identity/charge to which the image has been associated.
	Requested By:	Photo Manager / IMS
	Requested To:	NIA
	Input:	Image unique key, category and photo date along with Person or Charge ID.
	Output:	Person details including Name(s), gender, date of birth and physical descriptors. List of charges/summons the photo may be related to.
	Requested By:	Photo Manager / IMS
	Requested To:	NIA
	Input:	Confirm the image meta-data to NIA. Eg Identity and if relevant the charge/summons to which the image(s) have been loaded.
	Output:	None.
Retrieve single thumbnail photo	Purpose:	For an NZP core application to retrieve the most recent thumbnail, facial image for a known person or a photo set.
	Requested By:	NZP Core application
	Requested To:	Photo Manager / IMS
	Input:	Person unique key(s) and photo type / category. Charge/Noting/Licence unique key(s) where a specific set of photos are required.
	Output:	Image(s) and image meta-data.
Retrieve all thumbnail photo	Purpose:	For an NZP core application to retrieve the all thumbnail, facial image for a known person.
	Requested By:	NZP Core application
	Requested To:	Photo Manager / IMS
	Input:	Person unique key(s) and photo type / category.
	Output:	Image(s) and image meta-data.
Retrieve full size image	Purpose:	For a NZP core application to retrieve a fill size image for a known Image ID.

	Requested By:	NZP Core application
	Requested To:	Photo Manager / IMS
	Input:	Unique Person ID and Image ID
	Output:	Image and image meta-data.
Photo – Person associated is removed	Purpose:	Advise NIA that a photo(s) are held for the individual have been disassociated from the identity. NIA retains meta-data for a photo against the identity within NIA. This supports the request of a photo(s) from IMS and any identity management tasks that may require action within either/both IMS and NIA
	Requested By:	Photo Manager / IMS
	Requested To:	NIA
	Input:	Image unique keys and NIA unique keys.
	Output:	None
Identities merged within NIA	Purpose:	Advise IMS that two known identities have been merged as they relate to the same individual, the subordinate identity has a photo(s) within IMS.
	Requested By:	NIA
	Requested To:	Photo Manager / IMS
	Input:	NIA Identity unique key for the target Identity and the NIA Identity unique key for the subordinate Identity.
	Output:	None.
MOJ Transfer Charge	Purpose:	Advise IMS that the Ministry of Justice (MOJ) have transferred a charge from one identity to another. The transfer may be to another name for the same individual or a new individual.
	Requested By:	NIA
	Requested To:	Photo Manager / IMS
	Input:	Identity details form the old and new identity, and the charge group. .
	Output:	None.
Update Firearms Licence Details	Purpose:	Advise IMS of the most recent Firearms Licence details so that a replacement/updated Firearms Licence can be printed. Note – Card production is a separate process.
	Requested By:	NIA
	Requested To:	Photo Manager / IMS
	Input:	Full details for the licence and licence holder.
	Output:	None.
Lookup most recent Person details.	Purpose:	IMS requests the latest details for an identity associated to an Image(s).

	Requested By:	Photo Manager / IMS
	Requested To:	NIA
	Input:	Image and Identity keys. Charge/Noting/Licence unique key(s) where a specific set of photos are required.
	Output:	Person details including Name(s), gender, date of birth and physical descriptors.
Request Charge Group Status	Purpose:	Determine the status of a charge group. This is required to determine if an image can be used within some features of the application. eg Filler candidate of a Photo Line Up.
	Requested By:	Photo Manager / IMS
	Requested To:	NIA
	Input:	Image, Person and Charge Group unique keys
	Output:	Advise that at least one conviction is held for the details provided.

Note: This table outlines the general behaviour and information define within the existing interfaces. Full attribution, business rules, error handling need to be managed within the design of the future solution.

1.3.7 Interface to ABIS

There is no direct system to system interface between ABIS and Photo Manager/IMS. Livescan/ABIS capture images as part of the NZP arrest/charge process, these are exported to a shared folder and loaded into IMS using the same process as those captured by districts on digital cameras.

1.4 New interfaces

These features are not part of the current state but are considered within the scope of the project for delivery.

1.4.1 Image retention for Formal Photos.

A new interface transaction will be established triggered from NIA to IMS to manage the Image retention indicator for Formal Photos.

1.4.2 Load Formal Photo from ABIS

A new electronic process will pass ABIS NIST files from Livescan/ABIS into IMS. This will replace the existing process which loads an image from a system folder.

2 Solution Overview

2.1 The tenderer shall provide an overview of the solution being proposed, that describes:

2.1.1 Overall system architecture. The inclusion of any diagrams would be beneficial.

2.1.2 Major functional and technical components, features and integration points.

2.1.3 Interfacing capabilities and protocols.

2.1.4 Security control mechanisms.

2.1.5 Scalability of the solution.

2.1.6 Communication middle-ware required/supported, including wired and wireless local area and wide area networking protocols required or supported.

2.1.7 Preferred enterprise management tools (if any) and the roles such tools might play in the solution.

2.1.8 Additional hardware and software required to support the system.

2.1.9 Disaster Recovery.

2.1.10 Non production environments including any constants or limitations or restrictions that apply to them.

3 Solution Development

3.1 The tenderer shall describe their problem management, release management, and change management processes for the device and software.

3.2 The tenderer shall provide a change history of past releases over the last three years for the device and software with dates and descriptions of major functional and technical enhancements.

3.3 The tenderer shall provide an outline of the planned development and release schedule for the device and software up to and including the next 24 months, and what functional and technical enhancements are expected within those releases.

3.4 The tenderer shall describe their organisation's approach to supporting past versions of the software solution, and in assisting customers to migrate to new releases.

4 Flexibility

4.1 The tenderer shall describe how flexible the solution is to customise specific integration and export and import features/functions for NZ Police such that the solution can be upgraded easily, and with minimal impact and cost, to incorporate those Police specific features.

4.2 The tenderer shall describe how any features requested by NZ Police for their solution are made and released.

4.3 The tenderer shall describe any new function (including upgrades or new versions of their current device) which they are in the process of developing or have recently developed, if not yet available.

5 Deployment and support

5.1 The tenderer shall provide an overview that describes:

5.1.1 Proactive monitoring and support of the solution.

5.1.2 Approach to initial deployment of the solution

5.1.3 Approach to managing future releases within the production and non-production environments.

5.1.4 Outline the future roadmap for product delivery and development.

6 FUNCTIONAL REQUIREMENTS

6.1 Image Integrity - User Activity Log

ID	DETAIL
IU1	It is mandatory that the system(s) will provide a user activity log. This may include but is not limited to the following: • Date/time and user who imported, updated, enhanced an image; and entered or updated its associated metadata. • Date/time and user who destroyed an Image. • Date/time and user who added or removed an image from a watch list. • Date/time and user who created an electronic line-up or photobook • Date/time and user who used an image in a line-up, photobook or exported the image. • Date/time the user created, used in viewing an electronic photobook The user activity log is visible to authorised users within the application.
IU2	It is mandatory that a user may view the artefact related to the object/image that they are viewing.

6.2 Image Integrity – Image Alteration

ID	DETAIL
IA1	The original image(s) stored by the image management system cannot be altered and storage meets the recommendations below. It is mandatory that the images must be safeguarded against alteration of the original images. Outline how your solution provides this safeguard. References: http://www.anzpaa.org.au/ArticleDocuments/282/2013%20Australia%20and%20New%20Zealand%20Guidelines%20for%20Digital%20Imaging%20Processes.pdf.aspx http://www.anzpaa.org.au/about/general-publications/guidelines-for-digital-imaging-processes.
IA2	It is mandatory that a working copy of the original image will be the image used for enhancement purposes, and that a link between the working copy and original image will be held and evident.

6.3 Image Management

ID	DETAIL
IM1	It is mandatory that the system(s) has/have the capacity to use unique keys for accessing of or by other systems retaining these as metadata against an image(s).
IM2	It is mandatory that images held meet ANSI/NIST minimum standard. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-290e2.pdf https://fiswg.org/FISWG_CaptureAndEquipmentAssessmentForFRSystems_v1.0_2011_05_05.pdf
IM3	It is mandatory that an authorised user has/have the ability to multiple select / discard images (facial, SMT and clothing) prior to permanent storage in system. Eg re scan an original image that did not initially scan correctly.
IM4	It is mandatory that an authorised user has the ability to correct the metadata associated to an image.
IM5	It is mandatory that the system will retain the original image without compression, ensuring the storage of the best quality image.
IM6	It is mandatory that the system(s) has/have the ability to lock stored images, both the original and each subsequent working copy to prevent alteration.
IM7	It is mandatory that an authorised user has the ability to export stored images to external media.
IM8	It is mandatory that the system(s) has/have the ability to store the following as separate images: (i) Facial -frontal (ii) Facial - Profile (iii) Full Body (iv) SMT - Scars, Marks, Tattoos
IM9	It is desirable that the system(s) has/have the ability to store the following as separate images: (i) Clothing logo
IM10	It is mandatory that all images must have a unique reference number.
IM11	It is mandatory that authorised user may destroy an image or set of images, including the original. If the image has been used as a filler in the line-up the line-up is flagged to prevent being re-used. NOTE: S.34 Policing Act governs destruction of originals and associated working copy images (except for images used in a line-up) captured under section 32 and 33 of the Policing Act. Child Protection (Child Sex Offender Government Agency Registration) Act 2016 governs the destruction of originals and associated work copy images captured under this legislation.

IM12	It is mandatory that thumbnails are at 100w by 125h pixels and are stored in the Image Repository compressed using JPEG Sequential Baseline mode to a target size of between 4KB and 5KB. Number of resolution levels: The image shall be encoded using enough resolution levels to ensure that a thumbnail with max (width, height) <= 64 is available in the image. Example: a 640x480 image shall be encoded with 5 resolution levels, which enables sub-resolution decodes of 320x240, 160x120, 125x100 and 80x60.
IM13	It is mandatory that the system(s) incorporate(s) the ability to categorise images into logically partitioned repositories for the storage of images according to their category. (Formal, Missing Persons, Firearms Licence Holders, Suspect etc)
IM14	It is mandatory that the system(s) can import image(s) regardless of source. This includes, but is not limited to, images from the following sources: (i) Livescan/ABIS (ii) Digital cameras (iii) iPhone (iv) Still capture of frames from both analogue and digital video sources (eg CCTV and video camera footage) (v) Images produced by composite likeness software (vi) Scanning of any hard copy photograph, slide or negative (eg forged identification documents or developed 35mm film) (vii) Any other recognised industry standard image software format (eg BMP, JPEG, TIFF, PNG, etc). (viii) External interface/source system
IM15	It is mandatory that the system retains meta data for a Formal Photo. This information should include, but is not limited to: (i) Image Identifier (unique) (ii) Image Type (List) (iii) Photographing Officer Name (iv) Photographing Officer ID (v) Date Photo Taken (vi) Time Photo Taken (vii) Date Photo Entered (viii) Station where photo taken (ix) NIA Person ID and/or PRN

IM16	It is mandatory that the system retains meta data for a Formal Photo. This information should include, but is not limited to: (x) NIA (DocLoc) Case Number (xi) Image Identifier (unique) (xii) Image Type (List) (xiii) Photographing Officer Name (xiv) Photographing Officer ID (xv) Date Photo Taken (xvi) Time Photo Taken (xvii) Date Photo Entered (xviii) Station where photo taken (xix) Offence Type (List) (xx) TCN (xxi) NIA Person ID and/or PRN (xxii) Driver Licence Number
IM17	It is mandatory that the system retain meta data for a suspect image. This information should include, but is not limited to: (i) NIA (DocLoc) Case Number (ii) NIA Person ID (iii) Suspect Image Identifier Number (unique) (iv) Image Type (List) (v) Photographing Officer Name (vi) Photographing Officer ID (vii) Date Entered (viii) Station (where image captured) (ix) Offence Type (List) (x) Image enrolled by QID
IM18	It is desirable that suspect images may have a 'Time to Live' allocated. Once the Time to Live period has expired the images will be omitted from searches unless specifically requested.
IM19	It is desirable that the Time to Live parameter is configurable per suspect image but has an initial default value.
IM20	It is mandatory that when a suspect image is matched and positively identified then the system(s) provide(s) a function to receive the NIA recorded name and update the suspect record meta data.

IM21	It is mandatory that the system retain meta data for a Firearms Licence image. This information should include, but is not limited to: (i) NIA Firearms Case Number (sourced from NIA) (ii) Image Identifier (Unique) (iii) Firearms Licence Number (FLICNO) (sourced from NIA) (iv) Image Type (List) (v) Likeness Verification Officer's Name (vi) Likeness Verification Officer's ID (vii) Date Entered (viii) Station (Nearest Arms Office to the licence holders residence) (ix) Licence Type (sourced from NIA) (Multi Select List [as a dealer must also have a standard licence]) (A = Standard, D = Dealer) (x) Endorsement Type (sourced from NIA) (List of 9 and must be multi-select) (B = Pistol, C Collector/general, C Heirloom, C Memento, C Theatrical, C Museum, C Kea Gun, E = Military Style Semi-Automatic, F = Dealer) (xi) Licence Expiry Date (sourced from NIA) (xii) Licence Holder Postal Address (sourced from NIA)
IM22	It is mandatory that the system retain meta data for a missing person image. This information should include, but is not limited to: (i) NIA (DocLoc) Case Number (ii) Missing Person image Identifier (unique) (iii) NIA Person ID (iv) Image Type (List - include Other for medical images such as dental records) (v) Capture Officer's Name (vi) Capture Officer's ID (vii) Date Photo Taken (year) (viii) Date Image Entered (ix) Station Image Entered (x) Missing Category (NIA) (xi) Status (NIA Located field)
IM23	It is mandatory that Formal photo images must include a permanent retention indicator. This indicator is set & removed based on NIA details. The indicator may set when an image is imported or triggered by receipt of an interface transaction.
IM24	It is mandatory that an individual within IMS can have their information sealed by an authorised user.
IM25	It is mandatory that a Sealed Identity can be only be viewed or returned in a search result (recognition or metadata) by an authorised user.
IM26	It is desirable that one or more selected photos for an individual are available for import and enrol against a new identity.

6.4 Image –Import of non Livescan/ABIS

ID	DETAIL
IN1	It is mandatory that the system(s) provides an interface to import digital images from media sources.
IN2	It is mandatory that the system(s) provides an interface to acquire and scan images from TWAIN compliant sources such as Flat Bed Scanners.
IN3	It is mandatory that the system provide an interface to import digital images from a system folder.
IN4	It is mandatory that the system(s) has/have the ability to import and enhance both: (i) Black and white photographic images (ii) Colour photographic images
IN5	It is mandatory that the system(s) has/have the ability to execute the following steps within the Import process: (i) View images for quality assurance / quality control purposes (ii) Run a biometric search of existing repositories (iii) Source metadata from core NZP applications (iv) Classify SMTs within current operation (Police Structure) (v) Return metadata updates to the core NZP applications when required (vi) Create a thumbnail image (vii) Store image(s), including the original and working copies.
IN6	It is desirable that the system(s) has/have the ability to execute the following steps within the Import process: (i) Classify Clothing, logos and /or patterns within current operation (Police Structure)
IN7	It is mandatory that the system facilitates the import of working copy(ies) of facial frontal images in accordance with the ANSI/NIST Best Practice Recommendations by: (i) Assisting the user with centring and sizing the image correctly (with on-screen visual guidelines including crop and rotate capabilities) (ii) Providing a real time image preview in cropped ANSI/NIST compliant view layout (iii) Following import (and automatically cropping, if necessary) of the image with an aspect ratio of 1:1.25 for facial images. (iv) Following different formats to accommodate associated images and metadata.

IN8	It is mandatory that the system(s) has/have the ability to enhance/adjust working copy images during the import process and prior to permanent storage by: (i) Converting to grey scale (ii) Enhancing pixel by pixel (iii) Adjusting colour, colour saturation, colour hue. (iv) Size (v) Brightness (vi) Colour correction including red-eye (vii) Cropping for subject (viii) Orientation

6.5 Image – Input NIST from Livescan/ABIS

Livescan/ABIS capture biometric details within NIST file. Each of these files is made up the following:

(i) One ANSI/NIST Type-1 Transaction Information record

(ii) One ANSI/NIST Type-2 user-defined descriptive text record containing key charge meta-data (e.g. TCN) and other data required

(iii) One (or more if multiple images) can be captured per charge ANSI/NIST Type-10 facial & SMT image record, containing image meta-data and the JPEG compressed image as part of a JFIF file.

ID	DETAIL
IL1	It is mandatory that the system(s) provides an interface to import file(s) from Livescan/ABIS. Images are embedded within a NIST file. A NIST file may contain multiple images related to a Formal Photo. Livescan/ABIS provide a TCN Number as the unique reference.
IL2	It is mandatory that the system(s) has/have the ability to execute the following steps for the original image within the Import process: (i) View images for quality assurance / quality control purposes (ii) Source metadata embedded within or associated to the imported NIST file (iii) Run a biometric search of existing repositories (iv) Source metadata from core NZP applications (v) Classify SMTs within current operation (Police Structure) (vi) Return metadata updates to the core NZP applications when required (vii) Create a thumbnail image (viii) Store image(s), including the original and working copies.

IL3	It is desirable that the system(s) has/have the ability to execute the following steps for the original image within the Import process: (i) Classify Clothing logo and/or patterns within current operation (Police Structure)
IL4	It is mandatory that the image management system facilitates the use of working copy images in accordance with the ANSI/NIST Best Practice Recommendations by: (i) Assisting the user with centring and sizing the image correctly (with on-screen visual guidelines and pan, tilt, rotation and zoom capabilities) (ii) Providing a real time image preview in cropped ANSI/NIST compliant view layout (iii) Following import (and automatically cropping, if necessary) of the image with an aspect ratio of 1:1.25 for facial images (iv) Following different formats to accommodate images and associated metadata.
IL5	It is mandatory that the system(s) has/have the ability to enhance/adjust working copy images during the import process and prior to permanent storage by: (i) Converting to grey scale (ii) Enhancing pixel by pixel (iii) Adjusting colour, colour saturation, colour hue (iv) Size (v) Brightness (vi) Colour correction including red-eye (vii) Cropping for subject (viii) Orientation.

6.6 Biometric – Enrolment and Matching

ID	DETAIL
BE1	It is mandatory that the user can select any image retrieved by the biometric matching process and display all the details (both associated images and metadata) stored in any image repository for recognition search.
BE2	It is desirable that the user has the ability to control the number of images that are retrieved as the result of the biometric matching process within a configurable range for recognition search.
BE3	It is mandatory that the most likely matches are presented to the user ranked in descending order of match likelihood using an intuitive measure of confidence rating, which must show for recognition search.
BE4	It is mandatory that recognition matching can be performed across all compliant image repositories.
BE5	It is mandatory that an intuitive and easily operable manual or automated anchoring process be provided to ensure that the biometric algorithm is correctly applied to the image that is the subject of the enrolment, matching or search.

BE6	It is mandatory that the facial recognition matching can be performed for any newly acquired image, or previously enrolled image, against any image repository or repositories on an ad-hoc basis using a recognised and proven biometric algorithm.
BE7	It is mandatory that the facial recognition matching that is performed for any newly acquired image or previously enrolled image against any image repository or repositories is able to be done on a rules based method.
BE8	It is desirable that the SMT recognition matching can be performed for any newly acquired image, or previously enrolled image, against any image repository or repositories on an ad-hoc basis using a recognised and proven biometric algorithm.
BE9	It is desirable that the clothing symbol/pattern recognition matching can be performed for any newly acquired image, or previously enrolled image, against any image repository or repositories on an ad-hoc basis using a recognised and proven biometric algorithm.

6.7 Biometric – Auto Match on enrolment

ID	DETAIL
BA1	It is mandatory that the system(s) will perform automated matching of new images at the time enrolment against images stored in the Image repositories (rules apply) and watch list mechanism.

The following table describes the rules associated with BA1 above.

Repository		Auto match on enrolment
Formal Photos	Offender	All Repositories
	CPOR	All Repositories
	Returned Offenders	All Repositories
Voluntary		Offender, Suspect and Missing Person
Firearms Licence		All Repositories
Suspect		All Repositories
Missing Person		All Repositories

6.8 Watch List

ID	DETAIL
WL1	It is mandatory that the system(s) provide(s) for real-time watch list monitoring.
WL2	It is mandatory that the system(s) provide(s) the ability for an approved user to maintain a variable number of discrete watch lists
WL3	It is mandatory that when a match occurs on watch list image and a newly enrolled image, then a notification will be sent to the enrolling user and to the watch list entry requestor.
WL4	It is mandatory that an approved user may view a watch list.
WL5	It is mandatory that an approved user may remove a watch list, or watch list entry.

WL6	It is mandatory that all images added to a watch list have a 'Time to Live' associated with the watch list entry after which time the entry is automatically removed from the watch list.
WL7	It would be desirable that the Time to Live parameter is configurable per watch list entry but has an initial default value.
WL8	It is desirable that the threshold level for automated matching is configurable by image type.
WL9	When a new enrolling image is matched to a Missing Person image and positively identify then the system provides a function to notify the user enrolling the new image.

6.9 Firearms Licence update & card production

Production of a physical firearm licence cards occurs weekly and involves the following process steps:

1. NIA extract Firearms Licence data for licences that are to be produced.
2. Photo Manager / Image Management System imports the file.. For each licence that NIA has identified, the user visually verifies the IMS Firearms details against those from NIA. Verified licence details and images are extracted for card production.
3. Licence and images are transferred to the card provider (ABCorp).
4. IMS records the date/time the licence was extract to the card provider.

ID	DETAIL
FL1	It is mandatory that the system provide a process to receive licence details from NIA.
FL2	It is mandatory that the user verify the system(s) details for the Firearms against those imported from NIA.
FL3	It is mandatory that the Image for the licence card is extracted to the prescribed folder structure.
FL4	It is mandatory that the meta-data for card production is extracted to file in the format prescribed by the card provider. Currently this is a text file.
FL5	It is mandatory that the meta-data extract and images are transferred to the card provider.
FL6	It is mandatory that the system(s) produce a control report for the licence card production process.

6.10 Queries

ID	DETAIL
SR1	It is mandatory that the system(s) provide(s) the capability to carry out quality assurance/quality control images and metadata. Quality assurance is based on quality score for an enrolled image(s). The details may be searched/filtered by user, Station (location) and time period.
SR2	It is mandatory that searching can be conducted dynamically in real time using multiple fields.

SR3	It is mandatory that the user can select any record retrieved by the searching process and display all the details (both other images and metadata) stored on any of the system(s) repositories relating to that image(s).
SR4	It is mandatory that the system(s) provide(s) the capability to search and retrieve enrolled images based on metadata using text-based searches in conjunction with biometric, SMT and pattern recognition. The tenderer is to describe the search capabilities of the solution.
SR5	Common Search Criteria for all image database will include, but are not limited to the following fields: (i) NIA (DocLoc) Case Number (ii) Image Identifier (unique) (iii) TCN Number (LiveScan/ABIS) (iv) Name (First, Middle, Last) (v) NIA Person ID Number (vi) PRN (from NIA) (vii) Date of Birth (DOB) and Date Range (viii) Gender (ix) Age and Age Range (x) Height and Height Range (xi) Eye Colour with multiple selection (xii) Glasses (xiii) Hair Colour with multiple selection (xiv) Hair type (style) (xv) Hair length (xvi) Facial hair (xvii) Build with multiple selection (xviii) Ethnicity with multiple selection (xix) Photo Reference Number (data migrated from IMS) (xx) Image Category (List) (xxi) Date Photo Entered (xxii) Station where photo taken (xxiii) Optionally, any other Image management system search fields (xxiv) Offence Type with multiple selection (xxv) Charge Station with multiple selection (xxvi) Arrest Record (xxvii) Arrest Date and Date Range (xxviii) QID Livescan User or person capturing the image (xxix) Date image captured (xxx) Date image record modified (with details) (xxxi) Include expired suspect time to live images.
SR6	It is desirable that the user has the ability to control the number of images that are retrieved as a result of the searching process so that only images that match above a configurable matching threshold are displayed.
SR7	Common result set for search for all image databases should include but is not limited to the following fields: (i) Image set(s)

	(ii) Name (First, Middle, Last) (iii) Arrest Date (iv) TCN (v) Gender (vi) Ethnicity (vii) Age (viii) Date of Birth (DOB) (ix) Photo Reference Number (IMS) (x) PRN (xi) NIA Person ID Number.
SR8	It is desirable that the system(s) Results Set is returned with the best match first.
SR9	It is desirable that the system(s) initially group(s) all records for each person together in the Results Set and presents all previous records for the same person in reverse chronological order.
SR10	It is mandatory that one or more of the search results may be included in predefined output. Eg Flyer, photo book`

6.11 Flyer

ID	DETAIL
FY1	It is mandatory that the user can either print, or store as a secured Adobe ® PDF file, a 'flyer' for any selected image(s). Content is based on the configurable template(s).
FY2	It is desirable that the user can also enter information in a free-text field to be displayed on the flyer to detail the Reason for Interest in the person(s). This can be associated to an image or to the overall page.
FY3	It is mandatory that template(s) for one page flyer can be configured by an authorised user.

6.12 Photo Line-Up

A line up is a group of images (displayed on a single page) used to conduct a formal photo identification. The candidate for a Photo Line Up must be a specific and known individual.

At least 7 other photos along with the candidate image are shown to a witness with the Candidate's (suspect) image randomly placed. It must be placed differently for each witness and not be in first place. No names or means of identification must be shown to the witness.

Where the line-up includes a Police employee as a witness, at least 9 other photos along with the suspect image are shown to the witness.

The number of photos in a line-up can be varied between 8 and 20 in increments of 2.

ID	DETAIL
LP1	It is mandatory that a Photo Line-up contains Facial images only.

LP2	It is mandatory that a Photo Line-up production can be undertaken by any authorised user.
LP3	It is mandatory that the system(s) provide(s) the capability to create printed and electronic photo line-ups that are easy to present to witnesses in a printed format and electronic, and suitable for evidential purposes.
LP4	It is mandatory that any witness interaction with a prepared electronic photo line-ups, including the witness details and any selections made must be recorded
LP5	It is mandatory that the creation of a photo line-up can be initiated using an image retrieved from the Formal photo repository or sourced though any image acquisition This image is the Candidate photo.
LP6	It is mandatory that the eligibility for filler images be verified prior to use in a Photo Line Up. Eligibility for filler images: (i) Status check against core NZP systems (ii) Sourced from Formal photo repository and subject to Permanent Retention.
LP7	It is mandatory that all the images presented to the user as filler candidate for inclusion in a Photo Line-up are able to be retrieved from the Formal photo repository using physical attribute matching in conjunction with textual-based searching.
LP8	It is desirable that the user can select that all the images presented to the user as a filler for inclusion in a Photo Line-up are able to be retrieved from the Formal photo repository using the system's biometric facial recognition in conjunction with attribute matching and textual-based searching.
LP9	It is mandatory that the number of images in each created line-up be from a minimum of 8 photos to a maximum of 20 photos.
LP10	It is mandatory that the number of photos in a line-up be variable between 8 and 20 in increments of 2 (i.e. 14, 16, and 18).
LP11	It is mandatory that each line-up will have a unique automatically generated Line-up Reference Number
LP12	It is mandatory that the system prevent a user form including two images of the same person (NIA Person ID) within a Photo Line-up.
LP13	It is mandatory that the candidate photo of the line-up can be accommodated into the line-up in a random position amongst all the selected candidate filler images from the Formal photo repository.
LP14	It is mandatory that the candidate photo of the line-up cannot be placed in the first place in the line-up.
LP15	It is mandatory that the completed photo line-ups are able to be exported (produced) for witness viewing. Note the following preferred NZ Police export formats and media: (i) an electronic presentation template containing defined preamble slides and a single appropriately sized image per slide (ii) an electronic Photo Line Up stored as a secured Adobe ® PDF file comprising all images appropriately sized and spaced to fit neatly on A4 sheets (or A3 sheets) without any empty image slots

LP16	It is mandatory that when any line-up is produced that both a witness and police copy must be created together and be distinguishable by electronic filename and by Page Title.
LP17	It is mandatory that the line-up produced for witness viewing only has the sequence number of the image within the line-up clearly displayed against each image. In the case of electronic templates the line-ups must also contain the prescribed preamble slides, which must be maintainable by an authorised user.
LP18	It is mandatory that a copy for internal police use must always be produced in the one page Photo Line Up regardless of the format of the witness copy.
LP19	It is mandatory that the following Person related information from the Formal photo repository is clearly displayed under each image on the line-up for internal police use and Line-up related information is recorded and saved with each line-up: Person related detail: (i) Last Names, Givens names. (ii) NIA Person ID number (iii) Age (iv) Unique Image Reference Number (v) Photo capture date Line-up related detail: (vi) (DocLoc) Case Number (Optional) (vii) Requesting Officer's Name (Optional) (viii) Requesting Officer's ID (Optional) (ix) Creating member Name (x) Creating Member ID (xi) Date
LP20	It is mandatory that if the candidate image used for the line-up has been externally acquired, then the displayed metadata is enterable for use on the internal police copy.
LP21	It is mandatory that the system allows enhancement to any image within a line-up.
LP22	It is mandatory that any completed line-up can be saved to a central repository and can be re-opened for further line-up viewing or printing but cannot be modified.
LP23	It is mandatory that a completed and saved line-up can be used as the basis to create a new one with the candidate photo in a different place than the original saved line-up (re-shuffle). The user can request a number of different line-up versions up to a maximum of 7 that will result in this number of distinct randomly ordered line-ups being produced in which the candidate image is always positioned in a different place in each line-up for display to different witnesses. The production of each line-up can be recorded along with the position in which the candidate image was displayed. This would allow subsequent requests to produce further versions of a line-up to place the candidate image in a different position to any previous line-up version produced.
LP24	It is mandatory that the number of images retrieved and available for inclusion in the line-up is displayed to the user.
LP25	It is desirable that the creation of a photo line-up can be performed using intuitive single mouse click and keyboard controls such as the dragging and dropping of images selected for inclusion into the line-up.

LP26	It is mandatory that the candidate of the line-up is clearly displayed to the user at all times whilst filler images are being selected for inclusion in the line-up.
LP27	It is mandatory that the population of the electronic template is automated such that all the selected images are inserted into their corresponding locations in the template and the User has the ability to resize the image and use 'enhancement tools' including background change capability if required.
LP28	It is mandatory that the population of the electronic Photo Line Up is automated such that all the selected images are inserted into their corresponding locations on the sheet and the images are automatically spaced and sized

6.13 Photo Book

This function is the ability to create a collection of images based upon selected criteria. Identifying details for each subject in the photobook must be displayed.

Such a Photo Book may be all members of a particular gang; or all burglars or paedophiles in a particular area; or all Firearms Licence Holders in a particular town; or all Missing Persons in a Police District.

NZP do not use photo books for witness viewing.

ID	DETAIL
PB1	It is mandatory that the system provide the capability to create a printed photo book.
PB2	It is desirable that the system provide the capability to create an electronic photo book.
PB3	It is mandatory that the system(s) provide(s) the capability to create a title for each photo book.
PB4	It is mandatory that all the images presented to the user as individual as for inclusion in a photo book are retrieved from multiple databases in the system(s), using the systems' textual-based searching facilities and biometric/pattern matching.
PB5	It is mandatory that the images to be retrieved can be controllable by the user.
PB6	It is desirable that the population of the electronic template is automated such that all the selected images are inserted into their corresponding locations in the template and the images are automatically spaced and sized.
PB7	It is mandatory that once saved, the electronic Photo Book can be reopened, reviewed and may be printed by authorised users.
PB8	It is desirable that an electronic photo book can be copied and edited to create a new photobook.
PB9	It is mandatory that a partially completed photo books can be saved in draft format.
PB10	It is mandatory that the Images resulting from different search criteria retrievals can be used to complete the population of a photo book.
PB11	It is mandatory that each image will also display/print the individual's details.

6.14 Investigative Features

ID	DETAIL
IV1	NZ Police currently use FACES version 4 from IQ Biometrics to create composite likenesses of suspects and offenders. It is mandatory that the system must be able to import images that have been output from FACES, and use these as probe image in a recognition search.
IV2	It is mandatory that the system(s) provide(s) the capability for a user to view all images of a particular person, including historical images, and allow for all images to be selected and viewed, and printed.
IV3	It is mandatory that the system(s) must provide image enhancement capabilities for all types of image regardless of source.
IV4	It is mandatory that the system(s) must include(s) the ability to add or remove features such as facial hair, jewellery, glasses, scars, etc to assist in determining the likely current appearance of an individual
IV5	It is mandatory that the system(s) include(s) the ability to enhance poor quality images by sharpening details and zooming into areas on interest to assist with criminal investigations
IV6	It is mandatory that the system(s) include(s) the ability to accommodate receipt of image formats from a wide variety of industry sources (such as those that require Multiplex Drivers, those that require Codec software, MPEG, AVI files etc) and allows captured still images or frames to be loaded as JPEG files.

6.15 Reporting

ID	DETAIL
RP1	It is desirable that the system(s) is able to export data to Police's corporate reporting tool (SAS).
RP2	It is mandatory that the system(s) provide management reporting. This may include but is not limited to: (i) Count of Image enrolment (ii) Counts of Photo books produced (iii) Counts of Photo Line Up production (iv) Counts of recognition searches conducted, by type (v) Count of Firearms Licence card productions actioned (vi) User activity statistics (vii) Count of watch list hits Reports may be filtered/broken down by time period, NZ Police district/area/station, User who actioned, requesting user, result of line-up.
RP3	It is mandatory that the system(s) provide operational reporting. This may include but is not limited to: (i) Report of Image enrolment (ii) Report of Photo books produced (iii) Report of Line up production, including date shown to witness and if witness selected a candidate. (iv) Report of recognition searches conducted, including intelligence link. (v) Report of recognition search hit rates. (vi) Report of watch list. (vii) Error reporting, any images that could not be loaded.

	Reports may be filtered/broken down by time period, NZ Police district/area/station, User who actioned, requesting user, repository, image type
RP4	It is desirable that a user can create, customise, save and share a report / output. The tenderer is to describe how the solution supports users defining and running reports to meet their needs.

7 NON FUNCTIONAL

7.1 Performance

Category	Historic Records (Current)	Estimated Additional Records per Annum (Future)	Estimated Transactions Volumes	Desired Response Times
Image Management - Formal	1.5m from 800,000 individuals	50,000 per annum	Current Image retrieval requests from NZP core applications 60,000 per day. Note the 'Loads" volume is the same as the 'additional records, if previous column.	The retrieval of a thumbnail or full image to a NZP core application be returned within 100 milli seconds for 95 % of the requests (10 per second). The retrieval of a full set of thumbnails to a NZP core application be returned within 200 milli seconds for 95% of the requests (5 per second). It is desirable that an image can be loaded within 30 seconds. This would see minimal user interaction to complete the load. The steps to loading an image are: (i) View images for quality assurance / quality control purposes (ii) Run a biometric search of existing repositories (iii) Source metadata from core NZP applications (iv) Classify SMTs within current operation (Police Structure) (v) Return metadata updates to the core NZP applications when required (vi) Create a thumbnail image (vii) Store image(s), including the original and working copies. Solution response times for steps (i), (ii), (vi) and
Image Management - Suspect	N/A	7,500 per annum		
Image Management - Firearms Licence holders	245,000 at any one time	10,000 renewals per annum 9,500 new per annum 9,500 removed per annum.		
Image Management - Missing Persons	200	500 per annum		
Image Management – Child Protection (Child Sex Offender Register)	1,500	2,300 per annum		

Category	Historic Records (Current)	Estimated Additional Records per Annum (Future)	Estimated Transactions Volumes	Desired Response Times
				(vii) to be completed within 5 seconds (for each step).
Facial Recognition Search, Compare, Match and Report Excluding image load process.	Nil	At least 15,000 per annum	At least 15,000 per annum	All Search, Compare, Match, and Report transactions (including using multiple metadata fields) be completed within 5 seconds.
Photo line-up Production	12,000 (Time to prepare: 20 – 60 minutes)	15,000 per annum (Time to prepare: 10 minutes)	15,000 per annum	Solution response times for production of a Photo Line Up with no user selection (ie initial display of images) be completed within 5 seconds.
Scars Marks and Tattoos / Clothing Logos	Nil	30,000 (estimated)	30,000 (estimated)	All Search, Compare, Match, and Report transactions (including using multiple metadata fields) be completed within 5 seconds.

Notes:

1. These Records exclude capture of additional images which will arise from inter agency Identity Management work (Drivers licences, passports, etc.).
2. These Records are based on existing Police Processes, legislation changes will see future substantial increases

ID	DETAIL
NFP1	It is mandatory that the solution support 70 concurrent users located though out New Zealand.
NFP2	It is mandatory that the tenderer outline how they will support the performance requirements specified in the above table.
NFP3	It is mandatory that the tenderer outline what is required to scale the solution by: (i) Doubling (above numbers x 2) (ii) Tenfold (above numbers x 10).
NFP4	The tenderer is to provide the facial recognition and pattern search response times for their solution.
NFP5	The tenderer is to provide the response times for their solution for production of a Photo Line Up with no user selection (ie initial display of images).
NFP6	The tenderer is to provide the response times of their solution for biometric Searches on: (i) Facial frontal images

	(ii) SMT pattern matching.
NFP7	It is mandatory that patching must be managed in accordance with NZISM. https://www.gcsb.govt.nz/publications/the-nz-information-security-manual
NFP8	It is mandatory that, all images and metadata NOT subject to destruction in IM11 are retained permanently.
NFP9	It is mandatory that, unless deleted by an authorised user, the following data is retained permanently: (i) Images and associated meta-data (ii) Photo Line Ups (iii) Photo books
NFP10	It is mandatory that User Activity Logs be retained permanently.

7.2 Usability

Requirements that ensure the appearance of the solution conforms to the expectations of NZP organisation and its users.

ID	DETAIL
NFU1	The tenderer shall describe the user interface of the major components of their solution.
NFU2	It is desirable that the systems should be designed to minimise the number of screen interactions, key presses and clicks required by the User to perform the critical processes supported by the System.
NFU3	It is desirable that the user interface will use terminology that is consistent with the NZP core operational data set.
NFU4	It is desirable that the format of information will be consistent with NZP core operational data set. eg DOCLOC Case Number, 10 digit numeric is formatted nnnnnn/nnnn
NFU5	It is mandatory that the user interface will use NZ format date/time.
NFU6	It is mandatory that the documents will use NZ format date/time.
NFU7	It is mandatory that documents produced may include confidentiality or disclosure statement where specified. The content of the station must be configurable. Current statement is: "This document is distributed in confidence to members of New Zealand Police. Possession of this document without lawful authority or excuse is an offence against Section 61(A) of the Policing Act 1958."
NFU8	It is mandatory that documents produced may include Police branding, including headings and logo where specified.
NFU9	It is desirable that documents will use terminology that is consistent with the NZP core operational data set for headings and field labels.
NFU10	It is desirable that the user interface behaviour within the systems are to have standard Windows alternative keyboard shortcuts provided.

	Eg Tab between fields, tab on auto complete, Ctrl-S is save.
NFU11	It is desirable that the user interface support touch screen users.
NFU12	It is desirable that messages can be configured to be meaningful to NZP process and terminology.
NFU13	It is desirable that errors, warnings displayed to user must be in plain language and indicate appropriate action to be taken.

7.3 Product & User Environment

Requirements for the physical environment within which the solution will operate.

ID	DETAIL
NFE1	Users within the enterprise environment are geographically dispersed throughout the NZ
NFE2	Users of the Image Management features are based within the National Biometric Information office.
NFE3	Users of the Case Investigation features are located though out the country.
NFE4	It is mandatory that all NZP user access all solution components via the NZP enterprise network or NZP mobility network.
NFE5	NZP Users may access the NZP enterprise environment via remote access tools. Network support levels vary greatly depending on the user's actually physical location.
NFE6	User access to USB ports, DVD and external media is restricted. Permission is granted to a user via an established NZP process. It is mandatory that the solution does not assume that a user has access to an external media device.
NFE7	Users may access a folder(s) to load images that have been emailed, scanned or transferred for importing into the solution. Permission for folder address is granted to a user via an established NZP process. It is mandatory that the user will choose the folder(s) for saving or retrieving files (images, documents etc.).
NFE8	Users work on a managed desktop. The ability to manage, configure or install software the on a workstation is restricted. It is mandatory that the desktop components must be configured and packaged for installation via the established NZP distribution process.
NFE9	It is desirable that the solution should operate correctly where the (workstation) logged on user has no local admin or install privileges.
NFE10	It is mandatory that the application is used on Windows 8.1 and Windows 10 workstation, laptop or tablet.
NFE11	It is mandatory that the Web based application components must be compatible with IE11 and CHROME v54 – and subsequent product releases.
NFE12	It is desirable that data must be retained within NZ.
NFE13	It is mandatory that DR and production solution must be geographically dispersed.

NFE14	The solution design will be submitted to NZP design review process (TAG & TCF). The vendor will work with the NZP ICT Technical Owner to complete the necessary high level & detailed design. Note: Should part of or the whole solution see data retained outside of NZ, the complexity of gaining approvals and "Certificate and Accreditation" is greater.

7.4 Data & Image Format

ID	DETAIL
NFF1	The tenderer shall describe the image formats used during the load, storage and transmission of the images by and within the solution, and for the long term evidential storage including the following: (i) Whether the image format is proprietary or a widely supported standard format. (ii) Whether the image format uses lossless compression or lossy compression. (iii) What software is required to view, resize, export, compress or convert the images into a standard image format, such that: (1) The image can be viewed on a standard Police end user device without requiring the installation of any additional or specialised software. (2) The image conforms to the NZ e-GIF standard. (IV) Whether the image format incorporates any digital watermark mechanism that can be used to verify the image has not been subsequently tampered after capture.
NFF2	The tenderer shall provide minimum, maximum and recommended resolution digital images the solution is capable of capturing. (i) For each resolution include the number of pixels as width, height, and total number of megapixels (MP or Mpx) (ii) For each resolution provide an indication of the corresponding digital image file size (MB) in the image format native to the solution. (iii) For each resolution provide an indication of the corresponding digital image file size (MB) in the JPG image format (if different to the native format).
NFF3	The tenderer shall describe any secure long term storage options available or supported by the solution for retention of data and images form a period of seven (7) years while preserving the evidential trail.

7.5 Licensed Software

ID	DETAIL
NFL1	The tenderer shall describe how the solution (including software, hardware and services) will be licenced to NZ Police. The tenderer shall provide the following information: (i) Who owns any licenced components of the solution? (ii) If the tenderer is not the owner, the tenderer's interest and rights in the licenced components of the solution (e.g. exclusive distributor, accredited reseller/installer/support service provider etc.). (iii) Restrictions applied to the licenced component of the solution that will restrict or preclude NZ Police form having the software operated, supported, enhanced, modified or upgraded by. (1) NZ Police itself or (2) Any third party (eg an existing or future contractor of NZ Police). (iv) Escrow. It is desirable that the tenderer agree to NZ Police's access to, and free usage

		of, commercial solution if one of the following events occurs: (1) Company files for bankruptcy or ceases to operate (2) Software becomes unsupported without an upgrade path.
	(v)	Identify any solutions features that have a licence cost

7.6 Availability and Hours of Operation

Quantifies the necessary reliability of the solution and defines the expected hours of operation.

Terms:

- System failure – an outage or a fault with a severity that prevents the users form using the system in an operational capacity.

ID	DETAIL
NFH1	It is mandatory that images must be available to NZP operational applications seven days a week, 24 hours a day subject to agreed outages.
NFH2	It is mandatory that Facial Recognition features are available seven days a week, 24 hours a day subject to agreed outages.
NFH3	It is mandatory that SMT Recognition features are available seven days a week, 24 hours a day subject to agreed outages.
NFH4	It is mandatory that Case Investigation features must be available seven days a week, 24 hours a day subject to agreed outages.
NFH5	It is mandatory that Image Capture is available seven days a week, 24 hours a day subject to agreed outages
NFH6	It is mandatory that Query, View, Search using metadata and/or biometric criteria must be available seven days a week, 24 hours a day subject to agreed outages
NFH7	It is mandatory that the system is to be available 99.9% outside of the agreed outage window(s). 99.9% equates to 86.4 seconds a day, or 43 minutes a month or 8.77 hours a year.
NFH8	Routine outages must be scheduled between Sunday 06:00 and 08:00 NZ time.
NFH9	Following recovery, it is mandatory the maximum loss of data after recovery from a disaster (RPO) is not more than 4 hours.
NFH10	In the event of a system failure, it is mandatory that the system is restored within required recovery time after a disaster (RTO) for the solution of 8.77 hours.
NFH11	It is mandatory that recovery occurrences must not exceed 1 in any consecutive 12 month period.
NFH12	It is mandatory that the deliver an agreed backup plan, compatible with agreed SLA's, RTO and RPO.

7.7 Support and Monitoring

ID	DETAIL
NFS1	Helpdesk service is be provided to users of the product. This service is provided 24 x 7 via NZP Service Hub processes. NZP Service Hub operates 24x7, with teams based in Wellington and Auckland. Vendor support is communicated and managed via the NZP Service Hub.
NFS2	It is mandatory that the vendor provides support for the supplied products and services. The tenderer is to describe the options, including costing, for support: (i) Monday – Friday between the hours of 7am and 11pm NZ Time (ii) 24 hours a day, 7 days a week.
NFS3	It is desirable that support for the vendor supplied products and services must be responded to within 1 hour.
NFS4	Support tools or additional software required by the vendor or service agent to install, configure, support monitor the solution must be stated and approved as part of the overall solution design.
NFS5	It is mandatory that the tenderer provide proactive monitoring of the solution. Tenderer is to describe how this could be provided.
NFS6	It is mandatory that the tenderer provide monthly reporting on (i) Availability (i) Capacity (ii) Security (iii) Performance Tenderer is to describe an outline of the reporting to be provided.

7.8 Interfacing with adjacent systems

ID	DETAIL
NFI1	It is desirable that interfaces to NZP core systems via the NZP ESB, using web services.
NFI2	It is mandatory that the solution interfaces with NZP core systems to request & respond, send to or receive from core NZP systems, image and/or metadata. This may include but are not limited to: (iii) Merge of person details (iv) Issue or update of Firearms Licence details (v) Transfer of charge between persons (vi) Retrieve Person details (prisoner or firearms licence) (vii) Retrieve most recent Person details (viii) Retrieve charge group status (ix) Update from NZP Operational Reference data (x) Returning reference keys for image load and updates (xi) Retrieval of single thumbnail photo (person or photo reference) (xii) Retrieval of single full size photo (person or photo reference) (xiii) Retrieve all thumb-nails for a person/category(s) (xiv) Send removal of association between image and person (xv) Submit formal photo.

NFI3	It is mandatory that images provided to NZP core systems in: (i) JPG format and (ii) Associated meta data/reference keys (iii) Available as full image or thumbnail.
NFI4	It is desirable that the solution can import/load, NZP existing ABIS / Livescan facial images and metadata via a NIST file.
NFI5	It is desirable that the solution can import/load, NZP existing ABIS / Livescan SMT images and metadata via a NIST file.
NFI6	It is mandatory that the system(s) must interface to NZP Active Directory.
NFI7	It is mandatory that the system(s) must interface to NZP Exchange to send emails, both internally and externally to NZP.
NFI8	It is mandatory that the system(s) import a file of Firearms Licences from NIA for card production.
NFI9	It is mandatory that the system(s) export to file share the images and metadata for the Firearms Licence card producer.

7.9 Release & Deployment Management

ID	DETAIL
NFD1	It is mandatory that Software upgrades must be managed within an agreed release process.
NFD2	It is desirable that Enhancement requests can be submitted, applied and released within an agreed process
NFD3	It is mandatory that releases are acceptance tested by NZP prior to deployment into production.
NFD4	It is mandatory that deployment of the solution components to Acceptance Test / Pre-Production must be managed via NZP change management process.
NFD5	It is mandatory that deployment of the solution components to production must be managed via NZP change management process.
NFD6	It is mandatory that software deployed to NZP enterprise desktops (into production) must be packed by the managed desktop provider

7.10 Migration of existing data

ID	DETAIL
NFM1	It is mandatory that Image (JPEG) and associated metadata, including IMS photo reference number, be migrated from the existing photo management solution into the new solution.
NFM1	It is desirable that Images be migrated from ABIS/Livescan NIST files and submitted into a capture process within the new solution.

7.11 Reference Data

NZP core operational reference tables define attributes and associated values for information that is shared across multiple systems. Examples include: Hair Colour, Types of Clothing, Offence Codes, Court Outcomes, classification of SMT. These values are expected to change overtime, a start/end date is applied to each version of the attribute values.

Image & SMT management only, are attributes and associated value lists that are not shared outside the boundary of the proposed solution.

ID	DETAIL
NFB1	It is desirable that reference data that is shared or exchanged with NZP core operational systems will be sourced & maintained from the NZP core operational reference tables.
NFB2	It is desirable that individual entries within reference data tables will support multiple version based on an effective date. The date used within effective date validation will vary depending on the business process/form.
NFB3	It is allowable for reference data that is used for Image & SMT management only, may be managed by NZP Support Users directly within the solution.

7.12 Authentication & Authorisation

Authentication and authorisation of the users provide the ability to logon to the provided solution and gain rights to execute specific functions within the solution.

Terms:

- Authentication is the verification of a UserID & password to access the system.
- Authorisation is application of role based access control for an authenticated user.

ID	DETAIL
NFA1	It is mandatory that Users will be authenticated via NZP Active Directory, using NZP Enterprise userID & Password.
NFA2	It is desirable Authentication process will display the Code of Conduct - Acceptable Computer Use policy statement.
NFA3	It is mandatory that Users must be authorised to perform task/functions within the application that are associated with their role.
NFA4	It is desirable that User's application access *roles) will be controlled via NZP Active Directory.
NFA5	It is desirable that features will support single sign-on, users will be authenticated without re-entry of NZP Enterprise userID & Password.
NFA6	NZP application interfaces are trusted, specific users credentials are not required to initiate an interface transaction.

7.13 Security

ID	DETAIL
NFC1	Data Classification for the solution is "Restricted".
NFC2	It is mandatory that the transmission of user authentication details, such as user ID and password, over any network connect, must be secure and encrypted.

NFC3	It is mandatory that the authentication keys, such as passwords and encryption keys, when storied, are stored securely and never stored in clear text.
NFC4	The tenderer shall describe the access control mechanisms required/supported by each component'/function of the solution. Examples might be use of username/password or certificates.
NFC5	The tenderer shall describe the audit logging facilities included in the solution. This should include the points at which events are logged, what is recorded, where it is reported, what formats are used, how it is secured, and how this information is presented to auditors of the system.
NFC6	The tenderer shall describe how the solution ensures consistency and accuracy of system clocks across the various components that comprise the solution. Consistent and accurate system clocks ensure the integrity of audit trail and evidential trail.
NFC7	The tenderer shall describe any end point protection (including antivirus, anti-spyware, anti-malware, device port locking, and firewall), if any, is provided/supported by the solution.
NFC8	The tenderer shall describe what internet access, if any, is required for the solution.
NFC9	The tenderer shall describe how fixes and security patches are deployed and applied within the solution, including frequency.
NFC10	It is mandatory that the solution complies with the Certification and Accreditation requirements. This applies to both production and non-production environments.
NFC11	It is mandatory that all people accessing the system, including vendor project and support users, will be require a successful NZP Vetting prior to access being granted.
NFC12	It is mandatory that all people accessing the system, including vendor project and support users access the system via an individually issued NZP QID/password.
NFC13	It is mandatory that all people accessing the system, including vendor project and support users, comply with NZP rules and policies.
NFC14	It is desirable that the data is encrypted at rest.
NFC15	It is mandatory that the solution operates successfully in a firewalled network environment.

7.14 System Auditing

ID	DETAIL
NFG1	It is mandatory that activity (system and user) will be logged within the system. The tenderer is to describe who they record activity and transactions (User or system) within the solution.
NFG2	It is mandatory that the system Audit Logs will be available to NZP Assurance Group. The tenderer is to outline how the audit logs can be access and viewed by the NZP Security Team. Identifying any software required to enable this.
NFG3	It is desirable that the system integrate with current NZP SIEM solutions.

7.15 Testing & Training environments

ID	DETAIL
NFTE1	It is mandatory NZP Testing will be undertaken in a non-production environment. This includes interfacing to NZP test environments.
NFTE2	It is mandatory that Acceptance / pre-production deployment testing will be undertake in a non-production environment prior to deploying the solution or subsequent release into the production environment.
NFTE3	It is desirable that the Acceptance / pre-production environment be: (i) Production-like in configuration and resourcing (ii) Stable and subject to change management (iii) Integrated with (interface to) NZP core application testing environments. Eg NIA and Data warehouse, ABIS. (iv) Support 20 concurrent users.
NFTE4	It is desirable that System Test environment be available for functional fix-re-test and integration testing to Police system test environments. This is more volatile and with less rigid change control than the Acceptance / pre-production environment.
NFTE5	It is desirable that a Performance Testing be undertaken by the tenderer, and a report provided to NZP that demonstrates how the solution meets the performance requirements.
NFTE6	Defects will be managed via an agreed process.
NFTE7	It is mandatory that NZP will test releases of the product.
NFTE8	It is desirable that training will be undertaken in a non-production Training environment.
NFTE9	It is desirable that the Training environment will interface with NZP operational application training environments.
NFTE10	It is desirable that Training environment will be maintained and aligned with the production release/upgrade cycle, to support the ongoing training needs for the new staff and new application releases.
NFTE11	The tenderer shall outline how they support the non-production test and/or training environments both prior to the initial solution deployment and during the ongoing live of the solution: (i) Scheduled maintenance (ii) Availability and support (iii) Refreshing of data and synchronised with other systems

7.16 Testing

ID	DETAIL
NFTT1	It is mandatory that the tenderer complete a Factory Acceptance Test of the solution prior to handing to Police for Acceptance Test.
NFTT2	It is mandatory that the tenderer provide a report on the Factory Acceptance Test. This should include: (i) Test coverage (ii) Defects or issues not resolved.
NFTT3	It is mandatory that the tenderer provide evidence that the performance requirements are met by the solution.

7.17 Capabilities & Knowledge of Audience

ID	DETAIL
NFK1	It is desirable that Case Investigation features can be used without any specific training in the application.
NFK2	It is desirable Case Investigation training manual/user guide must be available to all users.
NFK3	It is mandatory that Image Management features are supported by a comprehensive training package. Initial training will be conducted on a single site.
NFK4	It is mandatory SMT Recognition features are supported by a comprehensive training package. Initial training will be conducted on a single site.

7.18 User Training

ID	DETAIL
NFUT1	It is mandatory that the tenderer provide the training for the following levels of users: (i) Help Desk Trainers - 2 ** (ii) Applications Support Group – 5 ** (iii) Productions Support Group - 5** (iv) Application Development Group - 3** (v) National work groups up to 15 users ** (vi) District Mentors (Train the trainer) up to 20 ** **Total number of trainees and roles to be trained to be confirmed. National work groups group includes National Biometrics Information team, Firearms Licensing and Missing Persons teams.
NFUT2	It is mandatory that NZ Police users will have access to self-paced learning material to ensure future training can be provided within Districts as and when required.
NFUT3	It is mandatory that the tenderer Training Deliverables include the following: (i) Skill and knowledge transfer (ii) System Administrations support skill transfer to appropriate agreed level (iii) Provide initial helpdesk knowledge base procedures.
NFUT4	It is mandatory that the tenderer provide the following Training Package: (i) Course overview, objectives and duration of the operational training that will be provided (ii) The expected training period for a general and a specialist user to become competent (iii) Hard and soft copy training documentation (iv) Scenarios and Hands-on exercises; required for District Mentors and administration personnel who will be operating the Image management system and peripheral equipment (v) Customised User Manual(s) (vi) Quick Reference Guide/s - including an overview of the key functions

	(vii) Modular presentation/demonstration (DVD) (viii) Online help (ix) FAQs (x) System Administration / Operations manuals (xi) Presentation and Demonstration.
NFUT5	It is mandatory that the tenderer Training delivered cover the following functionality: (i) formal photo line-up creation (ii) watch lists (iii) search facilities (iv) viewing images (v) biometric facial matching through facial recognition, and SMT matching (such as matching a suspect photo against a prisoner photo or a Facial composite photo against the known individual databases). (vi) reporting and presentation.
NFUT6	All appropriate documentation is available to be utilised on the NZ Police Standard Operating Environment. This includes, but is not limited to, being able to publish training and user documentation on the NZ Police Intranet and training support tools.
NFUT7	It is mandatory the tenderer supplied training of users is to be: (i) Provided in clear, comprehensible English (ii) Provided in a timely manner (iii) Comprehensive and complete, with appropriate level of detail (iv) User-friendly and effective in structure, format, duration and presentation.
NFUT8	It is desirable that the tenderer supply a softcopy of the training material without copyright so that it can be tailored to NZP training needs.

7.19 Project Management

ID	DETAIL
NFPM 1	The tenderer shall describe any Project Management, Software Development and System Support recognised standards they are audited and certified for (e.g. ISO/IEC, PRINCE2, CMMI, ITIL).
NFPM 2	The tenderer shall describe their standard Project Management approach, including the references and/or outlines of any frameworks and methodologies used.
NFPM 3	The tenderer shall summarise the qualifications and experience of their personnel in similar projects/deployments.
NFPM 4	The tenderer shall list describe their intended roles and involvement in this project.
NFPM 5	The tenderer shall describe how they intend to modify and customise their total solution to meet the requirements of this RFP.
NFPM 6	The tenderer shall outline the timeline required to implement the solution, including customisation and testing.

NFPM 9	The tenderer shall describe their intended approach towards long term proactive support and monitoring of the implemented solution, including but not limited to: (i) Support capabilities (Helpdesk) (ii) Location of their support services (iii) Capabilities for remote access and assistance (iv) Availability of support services (e.g. 24/7, work, hours, weekends etc.).
NFPM 10	The tenderer shall outline the approach the project will use to ensure quality control of the (i) Solution (ii) Project execution.

7.20 Police Deliverables

ID	DETAIL
NFPD1	The tenderer is to provide a details list of all requisite solution component specifications that are to be provided by Police in order for the System to operate in accordance with their proposal. The list should include but is not limited to hardware, software, cabling, interfaces, configurations, services, permissions, licenses and equipment.
NFPD2	The tenderer is to detail all assumptions that have been made in regard to any existing aspects of the Police ICT environment that are required in order for the system to operate in accordance with their proposal.

8 Future Strategic

The following may be required to support the future strategic of New Zealand Police. Describe how your solution will support each of the following requirements:

ID	DETAIL
FTR1	Facial Recognition capability to include using photos 'searched' from ABIS2 by an 'API' request via the Police ESB. Likely examples are ABIS2 connectivity to other Government agencies biometrics solutions for passport photos, drivers licence photos, etc.
FTR2	Ability for ABIS2 solution to automatically generate key image meta-data information, supplementing the meta-data manually captured. Likely example is 'red spider on neck' can be captured and is searchable. This may be occur during initial loading, but over time when more image patterns are quantified, these can be collected automatically against stored images.
FTR3	Ability to import CCTV feed into IMS, identify and image or images for recognition searching.
FTR4	Deliver functionality on an IOS mobility device.

END DOCUMENT

NEW ZEALAND POLICE

AND

[NAME OF SERVICE PROVIDER]

Ref: TN xxxx

MASTER ICT SERVICES AND DELIVERABLES AGREEMENT

(Draft)

New Zealand POLICE
Nga Pirihimana O Aotearoa

CONTENTS

AGREEMENT dated day of [month and year]

PARTIES

(1) **HER MAJESTY THE QUEEN IN RIGHT OF NEW ZEALAND** acting by and through the Commissioner of Police ("Police").

(2) **[Legal name of Service Provider] of [Registered address of Service Provider], (Service Provider)**

BACKGROUND

(a) Police wishes to engage the Service Provider to provide certain services and deliverables to Police.

(b) The services and deliverables will be provided to Police under Statements of Work entered into by the parties and governed by the terms and conditions set out in this agreement.

(c) The Service Provider has agreed to provide those services and deliverables to Police on the terms and conditions set out in this agreement, including each Statement of Work.

AGREEMENT

1. DEFINITIONS AND INTERPRETATION

1.1 **Definitions:** In this Agreement, the following terms have the following meanings unless the context requires otherwise:

Acceptance Certificate means, in respect of any Deliverable, a written notice from Police to the Service Provider substantially in the form attached as Schedule 4 recording that Police is satisfied that the Acceptance Criteria for the Deliverable have been met;

Acceptance Criteria means the following criteria:

(a) the relevant Deliverable complies with the Specifications;

(b) all warranties set out in clause 13 are true and correct in relation to the relevant Deliverable; and

(c) the relevant Deliverable complies with all acceptance criteria set out in the Statement of Work governing the supply of that Deliverable;

Acceptance Test Plan means the acceptance test plan recorded or specified in the relevant Statement of Work or, where no such acceptance test plan is recorded or specified in the Statement of Work, the acceptance test plan to be prepared by the Service Provider and approved by Police in accordance with clause 9.2;

Acceptance Tests means the acceptance tests recorded or specified in the relevant Statement of Work, or where no such acceptance tests are recorded or specified in that Statement of Work, the acceptance tests to be prepared by the Service Provider and approved by Police in accordance with clause 9.6;

Agreement means this agreement, the schedules to this agreement, all Statements of Work entered into under this agreement, the RFP and the Proposal;

Business Day means any day other than a Saturday, a Sunday or a public holiday (as defined in the Holidays Act 2003) in Wellington, New Zealand;

Change has the meaning given to that term in clause 8.8;

Change Control Process means the process set out in Schedule 3;

Commencement Date means the commencement date of this Agreement set out in Schedule 1;

Confidential Information means, in relation to a party, all information of any kind, whether written, electronic or otherwise, and whether marked or identified as being confidential, relating to that party or its business operations and, in relation to Police, includes the Police Data;

Control means, in relation to a party:

(a) the legal, beneficial or equitable ownership of at least 50% of the shares in that party;

(b) the power to appoint more than 50% of the board of directors of that party; or

(c) the power to control, by any other means, the affairs and policies of that party;

Crown means Her Majesty the Queen in right of New Zealand, including all:

(a) ministers of the Crown;

(b) government departments;

(c) offices of Parliament;

(d) Crown entities as defined in the Crown Entities Act 2004; and

(e) state enterprises as defined in the State-owned Enterprises Act 1986;

Deliverable means the System and all Equipment, Documentation, Software and other materials provided, or to be provided, by the Service Provider under or in connection with this Agreement, including all deliverables set out in Statements of Work entered into under this Agreement;

Delivery Notice has the meaning given to that term in clause 9.4;

Developed Software means the software developed, created or commissioned by the Service Provider or any other person under or in connection with this Agreement, including the software described as Developed Software in a Statement of Work;

Disclosing Party means the party disclosing the relevant Confidential Information under this Agreement;

Documentation means any document which the Service Provider must prepare or provide to Police in accordance with this Agreement and any other documentation reasonably required by Police to enable Police to use and obtain the full intended benefit of the Deliverables and the Services;

Encumbrance means a security agreement, debenture, mortgage, charge, pledge, lien, title retention, option, right of first refusal, right of pre-emption, any "security interest" as that term is defined in the Personal Property Securities Act 1999, and any other third party interest of any kind;

Error means, in relation to any Software, any failure of that Software at any time to:

(a) operate in good working order;

(b) comply with the Specifications for that Software or with any other requirements for that Software set out in the relevant Statement of Work; or

(c) comply with any of the warranties set out in clause 13.1(e) to (k);

Escrow Agreement has the meaning given to that term in clause 15.10(a);

Existing Material means all documentation, software and other materials used or provided by a party under or in connection with this Agreement that are:

(a) owned by, or licensed to, that party prior to the Commencement Date; or

(b) developed independently from this Agreement by that party,

and that are not developed, commissioned or created under or in connection with this Agreement and including, in the case of Police, all Police Property;

Equipment means any hardware to be supplied to Police under this Agreement as described in the Statement of Work;

Expiry Date means the expiry date set out in Schedule 1;

Fees means the fees set out in any or all Statements of Work, as the context requires;

Force Majeure Event means, in relation to either party (**Affected Party**), an event or circumstance beyond the reasonable control of the Affected Party, including:

(a) an act of God;

(b) an act of public enemy, or declared or undeclared war or threat of war; or

(c) a terrorist act, blockade, revolution, riot, insurrection, civil commotion or public demonstration (other than one caused by the Affected Party),

but not including any event or circumstance, or any failure to comply with any term of this Agreement, arising from such event or circumstance, that could have been avoided by the Affected Party's exercise of business continuity or other practices in accordance with best practice in New Zealand;

GST means goods and services tax payable under the GST Act at the rate prevailing from time to time, including any tax levied in substitution for that tax;

GST Act means the Goods and Services Tax Act 1985;

Intellectual Property Rights means all industrial and intellectual property rights whether conferred by statute, at common law or in equity, including all copyright, rights in relation to inventions (including all patents and patent applications), trade secrets and know-how, rights in relation to designs, rights in relation to trade marks, business names and domain names;

IP Claim has the meaning given to that term in clause 15.7(a);

Maintenance Release means any software released generally to users to replace, modify or attach to any software to rectify any Error, including releases which, in addition to rectifying an Error, provide additional functionality;

Mediation has the meaning given to that term in clause 18.1(b);

Mediation Notice has the meaning given to that term in clause 18.1(b);

Milestone means a milestone recorded in a Project Plan;

Milestone Date means a date by which a Milestone must be achieved, as specified in a Project Plan;

New Release means any Maintenance Release or New Version;

New Version means any new version of software released generally to users to replace, modify or attach to any software to provide additional functionality, not being a Maintenance Release;

Notice has the meaning given to that term in clause 20.9;

OIA means the Official Information Act 1982;

Personnel means any employee, agent or representative of the Service Provider, or of any subcontractor of the Service Provider, who provides any Service or Deliverable;

Police Data means all information relating to Police, its business strategies, marketing plans, facilities, systems, technologies, stakeholders, customers, suppliers or third party service providers;

Police Property means equipment, tools or other property owned or leased by Police or any Related Party;

Police Requirements means the requirements for the Deliverables and Services set out in the relevant Statement of Work;

Police Sites means the sites specified by Police from time to time at which the Service Provider will provide the Services or Deliverables;

Project Delay has the meaning given to that term in clause 8.5;

Project Manager has the meaning given to that term in clause 7.1;

Project Plan means a project plan set out or described in a Statement of Work;

Proposal means:

(a) the Service Provider's proposal (if any) described dated 2/9/2010; and

(b) any other proposal submitted by the Service Provider in response to any other request for proposal for Services or Deliverables released by Police, together with any written material provided to Police by the Service Provider to supplement, explain or expand on that proposal;

Proprietary Software means the software described in a Statement of Work which is owned by the Service Provider or any third party;

Public Safety Organisations means organisations and agencies present at Police Sites that who engaged in public health or public safety activities from time to time, including:

- New Zealand Fire Service
- Victim Support
- D.A.R.E.
- Bluelight
- Neighbourhood Support
- Community Patrols

Receiving Party means the party receiving the relevant Confidential Information under this Agreement;

Records means information, whether in its original form or otherwise, including a document, a signature, a seal, text, images, sound, speech, or data compiled, recorded, or stored, as the case may be:

(a) in written form on any material;

(b) on film, negative, tape, or other medium so as to be capable of being reproduced; or

(c) by means of any recording device or process, computer or other electronic device or process;

RFP means the request for proposal TN[xxxx] advertised by Police on [date/month/year];

Service Levels means the standards of service specified in this Agreement, including the service levels specified in the relevant Statement of Work;

Services means:

(a) the services described in this Agreement, including in each Statement of Work;

(b) all services incidental to, or required for the proper performance of, the services described in (a); and

(c) all other services agreed in writing by the parties from time to time;

Software means the Developed Software and the Proprietary Software and all other software which is provided by the Service Provider to Police under this Agreement;

Source Materials means the source code, algorithms and all other information, materials and documents necessary to enable a reasonably skilled person to maintain, amend and enhance the relevant software without reference to any other person or document and whether in eye-readable or machine–readable form;

Specifications means, for each Deliverable, all the specifications and requirements relevant to that Deliverable including all the specifications and requirements for that Deliverable set out in:

(a) the relevant Statement of Work, and

(b) the RFP and the Proposal to the extent that they are not inconsistent with the specifications under paragraph (a) of this definition.

Specified Personnel means the Personnel specified in the relevant Statement of Work;

Statement of Work means a statement of work entered into under this Agreement substantially in the form set out in Schedule 2;

Statement of Work Start Date means the start date for the applicable Statement of Work, as set out in the Statement of Work;

Statement of Work Term means the term of the applicable Statement of Work, as set out in the Statement of Work;

System means the Deliverables supplied under this Agreement and all existing equipment, software and cabling owned or used by Police to which the Deliverables are to be connected, or integrated, working in combination together to meet the Specifications;

Term means the term of this Agreement described in clause 17;

Train the Trainer means the training of not less than two but no more than five Police staff in the use and operation of a New Release; and

Valid Tax Invoice has the meaning given to the term in clause 11.3.

1.2 **Interpretation:** In this Agreement, unless the context requires otherwise:

(a) headings are for convenience only and have no legal effect unless otherwise specified;

(b) references to the singular include the plural and vice versa;

(c) references to a party include that party's successors, executors, administrators and permitted assignees (as the case may be);

(d) references to clauses and Schedules are to the clauses and Schedules in this Agreement;

(e) where a word or phrase is defined, its other grammatical forms have a corresponding meaning;

(f) references to a person include:

(i) an individual, firm, company, corporation or unincorporated body of persons;

(ii) any public, territorial or regional authority;

(iii) any government; and

(iv) any agency of any government or authority;

(g) an obligation not to do anything includes an obligation not to suffer, permit or cause that thing to be done;

(h) references to any statute include any amendment to, or replacement of, that statute and any subordinate legislation made under it;

(i) wherever the words "includes" or "including" (or similar words) are used, they are deemed to be followed by the words "without limitation";

(j) except as otherwise expressly stated, monetary references are references to New Zealand currency; and

(k) if there is any conflict between the terms of this Agreement, the following order of precedence will apply, unless otherwise expressly specified to the contrary in this Agreement (including in a Statement of Work):

(i) the terms of the body of this Agreement;

(ii) the Schedules to this Agreement;

(iii) the terms of each Statement of Work;

(iv) the RFP; and

(v) the Proposal.

2. APPOINTMENT

2.1 **Appointment:** Police appoints the Service Provider, and the Service Provider agrees, to provide the Services and Deliverables to Police on the terms and conditions of this Agreement.

2.2 **Non-exclusive appointment:** The parties agree that:

a) the Service Provider's appointment under this Agreement is non-exclusive; and

b) Police may appoint third parties to provide services or deliverables similar to, or identical with, the Services or Deliverables at any time, or may provide them itself.

2.3 **No minimum level of business:** Police does not guarantee any minimum level of business by entering into this Agreement.

2.4 **Reliance:** The Service Provider acknowledges that Police is relying on the Service Provider's expertise in entering into this Agreement, including all statements made by the Service Provider in the Proposal or in any written material provided to Police regarding the Service Provider's or the Personnel's skills, experience and expertise and the quality and performance of the Services and Deliverables.

3. STATEMENTS OF WORK

3.1 **Police request:** From time to time Police may seek proposals from the Service Provider for the provision of services or deliverables or both.

3.2 **Service Provider response:** The Service Provider agrees to respond to Police's requests under clause 3.1 within a reasonable time and in each case to provide a proposal containing:

(a) a description of the Services and Deliverables to be provided by the Service Provider;

(b) details of the Service Provider's Fees for those Services and Deliverables which must comply with the principles in clause 5(c) of Schedule 3; and

(c) all other information reasonably requested by Police relating to those Services and Deliverables.

3.3 **Negotiate Statement of Work:** Following receipt of the Service Provider's proposal under clause 3.2, Police may accept, reject or request changes to the proposal and the Service Provider will make any changes reasonably requested by Police.

3.4 **Enter into Statement of Work:** Once the parties have agreed the terms on which the Service Provider will provide the Services and Deliverables sought by Police under clause 3.1, the parties will enter into a Statement of Work for those Services and Deliverables substantially in the form of Schedule 2 provided that, until such time as a Statement of Work is signed by the parties, Police will not be obliged to pay any Fees in respect of those Services or Deliverables.

4. SERVICE PROVIDER'S OBLIGATIONS

4.1 **Performance:** In providing the Services and Deliverables and complying with its other obligations under this Agreement, the Service Provider must:

(a) provide, at its own cost, all equipment, tools, materials and other resources necessary for the provision of the Services and Deliverables;

(b) take full responsibility for the performance of all tasks and activities necessary to provide the Services and Deliverables in accordance with this Agreement, other than tasks or activities specifically identified as being Police's responsibility;

(c) comply with all reasonable directions given by Police from time to time;

(d) comply with all Police policies and procedures notified to the Service Provider from time to time;

(e) comply with all of its legal obligations (including under statute, regulation, and contract);

(f) co-operate with Police and all other contractors and service providers to Police, to ensure the Services, Deliverables and all products and services related to them are delivered efficiently and seamlessly to Police;

(g) not damage, disrupt, introduce any computer virus into or otherwise adversely affect any part of Police's:

(i) business or operations; or

(ii) information technology or telecommunications systems; and

(h) promptly notify Police in writing of:

(i) any breach of the Service Provider's obligations under this Agreement; and

(ii) any matter that may impact on the Service Provider's ability to perform its obligations in accordance with this Agreement.

4.2 **Service Levels:** The Service Provider must provide the Services and Deliverables so as to meet or exceed the applicable Service Levels.

4.3 **Failure to meet Service Levels:** Without limiting Police's other rights and remedies, if the parties agree that Police is entitled to rebates from the Fees paid or payable under this Agreement if the Service Provider fails to meet any Service Level, details of those rebates and the methods of calculating and paying them will be described in the relevant Statement of Work. Further, the Service Provider will implement relevant service improvement plans to ensure that the Services that have failed Service Levels are continuously improved.

4.4 **Maintain reputation:** The Service Provider must not engage in any activity or conduct that might, in Police's opinion, damage the reputation or image of Police or the Crown.

4.5 **Conflict of interest:** The Service Provider must not enter into any agreement or arrangement that will, or is likely to:

(a) prejudice the Service Provider's ability to meet its obligations under this Agreement; or

(b) create a conflict of interest for the Service Provider.

4.6 **Resolve conflict:** Notwithstanding clause 4.5, the Service Provider must:

(a) immediately notify Police in writing if the Service Provider is, or is likely to be, conflicted in the performance of its obligations under this Agreement; and

(b) take all actions reasonably required by Police to resolve any such conflict.

4.7 **Add value:** The Service Provider must proactively use its experience and expertise to improve the Services and Deliverables, and the manner of providing them, to more effectively and efficiently meet Police's requirements both in terms of quality and cost.

5. POLICE'S PROPERTY AND SITES

5.1 **Police Property:** If the Service Provider has access to any Police Property under or in connection with this Agreement, the Service Provider must:

(a) use the Police Property:

(i) for the sole purpose of complying with its obligations under the relevant Statement of Work and for no other purpose; and

(ii) only to the extent necessary to comply with its obligations under the relevant Statement of Work;

(b) comply with all directions regarding the use of Police Property given by Police from time to time; and

(c) return all Police Property to Police on the earlier of:

(i) completion of the Services or Deliverables relating to that Police Property;

(ii) receipt of Police's request for it to be returned; and

(iii) termination or expiry of the relevant Statement of Work.

5.2 **Police Sites:** Police will provide the Service Provider with access to the Police Sites solely for the purpose of enabling, and to the extent necessary to enable, the Service Provider to comply with its obligations under the relevant Statement of Work. The Service Provider must not use or access the Police Sites or any other premises of Police for any other purpose without Police's prior written consent.

6. PERSONNEL AND SUBCONTRACTORS

6.1 **Personnel:** The Service Provider:

(a) must ensure the Services and Deliverables are provided using appropriately experienced, skilled and qualified Personnel who are capable of providing the Services and Deliverables to the standards required under this Agreement;

(b) is responsible for all acts and omissions of the Personnel as if they were the acts or omissions of the Service Provider; and

(c) must ensure that all Personnel comply with the terms of this Agreement and with all of Police's policies, procedures and directions;

(d) shall not employ any person or contractor to perform its obligations under this Agreement who is not prepared to undergo a security check by Police or who has not been approved by Police under sub-clause (c). Subject to its security requirements, Police shall advise of the form of such security check (including the information that will be required by Police, the use that will be made of that information, whether than information will be retained by Police, and if so, for how long it will be retained), which shall comply with the provisions of the Privacy Act 1993;

(e) will promptly upon request from Police obtain written consent from the employee or contractor to supply Police with such personal details to enable a security check to be carried out;

(f) will forward those details to Police and will not engage an employee or contractor to perform the Services until Police's written approval of the security check results has been obtained;

(g) the services shall be provided solely by those persons approved by Police under this clause 6. If any such persons become unavailable or refuse to provide the Services or do not meet the security standards required by Police, shall nominate a replacement person or persons within seven (7) days. The provisions of this clause shall also apply to such proposed replacement;

(h) shall ensure that each of its personnel engaged in providing the Services shall if requested by Police execute and otherwise comply with the terms of a confidentiality deed in a form agreed by the parties.

6.2 **Specified Personnel:** The Service Provider must ensure the Specified Personnel provide the Services and Deliverables they are required to provide under the relevant Statement of Work. The Service Provider may only replace any Specified Personnel if:

(a) that person is unavailable due to resignation, illness or death;

(b) the replacement person is, in the reasonable opinion of Police, appropriately experienced, skilled and qualified to perform the applicable role; and

(c) the Service Provider first obtains Police's written consent to the replacement person, such consent not to be withheld unreasonably.

6.3 **Subcontractors:**

(a) The Service Provider must not subcontract any of its obligations under this Agreement to any other person without first obtaining Police's written consent and complying with clause 6.3(b).

(b) The Service Provider must:

(i) ensure each subcontractor complies with the terms of this Agreement;

(ii) manage the agreement between the Service Provider and the subcontractor in the best interests of Police;

(iii) authorise Police to deal with the subcontractor directly;

(iv) ensure that an appropriate written agreement is in place between the Service Provider and the subcontractor that is consistent with the terms of this Agreement; and

(v) if requested by Police, ensure that the agreement referred to in clause 6.3(b)(iv) acknowledges the benefit to Police for the purposes of the Contracts (Privity) Act 1982 and is therefore enforceable by Police.

(c) The Service Provider will remain liable to Police for all acts or omissions of each subcontractor as if they were the acts or omissions of the Service Provider. The entry by the Service Provider into an agreement with a subcontractor will not:

(i) create a contractual relationship between Police and the subcontractor except as described in clause 6.3(b)(v); or

(ii) relieve the Service Provider from liability for the performance of any obligations under this Agreement.

(d) The Service Provider must obtain Police's prior written consent to the replacement of any subcontractor, and clauses 6.3(b) and (c) will apply to all replacement subcontractors.

6.4 **Health, safety and security:** The Service Provider will comply, and will ensure that all of its Personnel comply, with all of Police's health, safety, operational and security requirements while on Police Sites and any other Police premises.

6.5 **Replacement of Personnel:** If Police considers (acting reasonably) that any of the Personnel are unsatisfactory or unsuitable then, without limiting any other rights of Police, Police may, by written notice, require the Service Provider to replace the relevant Personnel and the Service Provider will do so as soon as possible at its own cost, but in any event no later than five Business Days after receipt by the Service Provider of the notice. In the case of any replacement of Specified Personnel, clauses 6.2(b) and (c) will apply.

6.6 **Non-solicitation:** Each party agrees not to actively solicit for employment during any Statement of Work Term any employee of the other party who has been engaged by the other party in connection with the System, Deliverables or Services. This clause does not prevent the a party from employing any person who responds to a genuine public advertisement placed by that party. If a party breaches this clause that party shall pay to the other by way of compensation 15% of the salary of the relevant employee for the first 12 months of the employee's employment by the breaching party.

7. PROJECT MANAGEMENT, REVIEWS AND REPORTING

7.1 **Project Managers:** Each party will appoint a project manager in relation to each Statement of Work (Project Manager) who will:

(a) serve as the primary point of contact with the other party; and

(b) have overall responsibility for the performance of that party's obligations under this Agreement.

The Service Provider's proposed Project Manager will be subject to the prior written approval of Police.

7.2 **Replacement:** Each party may replace its Project Manager from time to time provided, in the case of Police, it gives prior written notice of such replacement and, in the case of the Service Provider, it complies with clause 6.2.

7.3 **Meetings:** The Project Managers will meet together in the manner and at the frequency specified in each Statement of Work and as otherwise reasonably required by Police, to:

(c) monitor progress of the Service Provider in providing the Deliverables and the Services;

(d) review resource needs and detail timing for upcoming tasks;

(e) as far as they are able, settle and agree any issues arising in the course of providing the Deliverables or the Services, and review risks and agree risk management actions;

(f) monitor compliance by each party of any other of their respective obligations under this Agreement;

(g) review and discuss system performance, efficiency systems planning, systems management and metrics; and

(h) monitor the Change Control Process and, where appropriate, software release management planning.

7.4 **Reporting:** The Service Provider must provide reports at the frequency and containing the detail set out in the relevant Statement of Work.

7.5 **Relationship meetings:** Each party will appoint appropriate relationship managers who will meet together, at no less than quarterly intervals, to:

(i) monitor compliance by each party of their respective obligations under this Agreement including performance against Service Levels; and

(j) discuss at a high level the business direction of each party and Police's existing and future requirements.

8. IMPLEMENTATION

8.1 **Delivery:** The Service Provider will deliver each Deliverable to the relevant Police Site in accordance with the relevant Statement of Work.

8.2 **Installation and implementation:** Unless otherwise agreed under a Statement of Work, the Service Provider will provide installation and implementation services in respect of all Deliverables in accordance with the requirements set out in the relevant Statement of Work or, if no such requirements are specified, in accordance with the reasonable timeframes and other requirements specified by Police.

8.3 **Project Plan:** The Service Provider will provide the Deliverables and the Services in accordance with the Milestones and other timeframes recorded in each Project Plan. Where no Project Plan is recorded in the Statement of Work, unless otherwise agreed in writing by Police, the Service Provider will, in accordance with the reasonable timeframes and other requirements specified by Police, prepare, and obtain approval from Police of, a project plan which records all of the details which this Agreement anticipates will be included in such project plan, including relevant milestones and the date by which each milestone must be achieved, and that approved plan will be taken to be the Project Plan for the relevant Deliverables and Services.

8.4 **Completion of Milestones:** Each Milestone in a Project Plan is complete when Police has advised the Service Provider in writing that Police is satisfied (acting reasonably) that the Service Provider has successfully completed that Milestone in accordance with that Project Plan.

8.5 **Failure to complete Milestones:** Without limiting any other rights or remedies of Police but subject to clause 8.6, if the Service Provider fails, or is likely to fail, to complete a Milestone by the relevant Milestone Date (a **Project Delay**):

(a) the Service Provider will, immediately following it becoming aware of the Project Delay, provide full details of the Project Delay to Police in writing;

(b) the Service Provider will (at its own cost) immediately take all steps available to it to avoid and minimise the effects of the Project Delay;

(c) the parties will, if requested by Police, meet to review in good faith the reasons for the Project Delay;

(d) the Service Provider will, if requested by Police, promptly prepare a comprehensive rectification plan setting out how it intends to complete the relevant Milestone, the relevant timeframes for such completion and any other details reasonably required by Police, and will submit such plan to Police for approval; and

(e) the Service Provider will, if requested by Police, comply with any rectification plan submitted by the Service Provider under clause 8.5(d), together with any modifications to the rectification plan or other requirements notified by Police.

8.6 **Project Delay caused by Police:** Where a Project Delay is caused by Police:

(a) the Service Provider will, immediately following it becoming aware of the Project Delay, provide full details of the Project Delay to Police in writing;

(b) the parties will, if requested by Police, meet to review in good faith the reasons for the Project Delay;

(c) the Service Provider will, if requested by Police, cooperate with Police in relation to the Project Delay and will use reasonable efforts to rectify the Project Delay and ensure future Milestone Dates are met, subject to the Change Control Process; and

(d) if, notwithstanding the Service Provider's compliance with clauses 8.6(a), (b) and (c), the Service Provider fails to complete the relevant Milestone by the relevant Milestone Date, the Service Provider will not be liable for that failure to the extent the failure was caused by Police.

8.7 **Extension:** Police may extend one or more Milestone Dates at any time by giving notice in writing to the Service Provider.

8.8 **Change Control Process:** If:

(a) Police requires any new deliverables or services under a Statement of Work that are not within the scope of that Statement of Work; or

(b) either party proposes any change to the Services and/or the Deliverables (including any changes to the nature or scope of the Deliverables or the Services or to the timing of the delivery of the Deliverables or the Services) and such change cannot be accommodated by another process in this Agreement,

(**Change**) the parties will comply with the Change Control Process in respect of each such Change. Any Change will not be effective until it is documented as an express variation to this Agreement.

8.9 **Risk and title:** Except as expressly specified in a Statement of Work:

(a) Risk in the Equipment shall pass on the issue of the Acceptance Certificate for the relevant Deliverables.

(b) Title in the Equipment passes to Police on payment for the Equipment and shall be transferred with clear title free from any Encumbrance.

9. ACCEPTANCE TESTING

9.1 **Applicability of Acceptance Tests:** The parties acknowledge that the process set out in this clause 9 will apply to all Deliverables except those that the parties have agreed in any Statement of Work will not be subject to any acceptance testing process.

9.2 **Acceptance Test Plan:** Each party will comply with its obligations set out in each Acceptance Test Plan at its own cost. Where no Acceptance Test Plan is recorded or specified in a Statement of Work, the Service Provider will, if requested by Police and in accordance with the reasonable timeframes and other requirements specified by Police, prepare, and obtain approval from Police of, an acceptance test plan which records all of the detail which this Agreement anticipates will be included in such acceptance test plan.

9.3 **Initial testing:** The Service Provider will, prior to the delivery of any Deliverable to Police, test the Deliverable in the manner described in the Acceptance Test Plan to determine whether or not the Acceptance Criteria for that Deliverable have been met.

9.4 **Delivery Notice:** The Service Provider will, upon completion of the testing described in clause 9.3 and the Service Provider being satisfied (acting reasonably, given its specialist expertise and experience) that the Acceptance Criteria have been met for the Deliverable, issue to Police a delivery notice **(Delivery Notice)** confirming that the Acceptance Criteria are met.

9.5 **Acceptance Tests:** Police will, following receipt of the Delivery Notice or the Deliverable as the case may be, conduct the Acceptance Tests for the relevant Deliverable in accordance with the Acceptance Test Plan. This testing may involve testing the Deliverable individually or in conjunction with other Deliverables or in conjunction with Police's other systems, as specified in the Statement of Work. The Service Provider will provide such assistance as is reasonably required by Police in relation to the Acceptance Tests.

9.6 **Truncated Acceptance:** Where no acceptance tests for the relevant Deliverable are recorded or specified in the Statement of Work or where Police otherwise requires a truncated acceptance process, the Service Provider will, in accordance with the reasonable timeframes and other requirements specified by Police, prepare, and obtain Police's approval of, acceptance tests for such Deliverable and Police will conduct those tests. Such acceptance tests must, at a minimum, be sufficient to demonstrate whether or not the relevant Deliverable meets the Acceptance Criteria for that Deliverable and may involve testing the Deliverable individually or in conjunction with other Deliverables or in conjunction with the Police System.

9.7 **Successful completion:** If the Acceptance Tests demonstrate to the satisfaction of Police (acting reasonably) that the Acceptance Criteria for the relevant Deliverable have been met, Police will complete and sign and provide to the Service Provider an Acceptance Certificate for that Deliverable substantially in the form attached as Schedule 4.

9.8 **Unsuccessful completion:** If the Acceptance Tests carried out under clauses 9.5 or 9.6 do not demonstrate to the satisfaction of Police (acting reasonably) that the Acceptance Criteria for the relevant Deliverable have been met, Police will notify the Service Provider of such failure within 10 Business Days of completion of the relevant Acceptance Tests and the Service Provider will, at its own cost and within 10 Business Days of receiving such notification from Police (unless otherwise agreed by the parties in writing), remedy any relevant failures or deficiencies so that the Acceptance Criteria are met.

9.9 **Repeat Acceptance Tests:** The Service Provider will immediately notify Police in writing when it has completed the remedial work under clause 9.8 and Police will, promptly after receipt of such notification, repeat the Acceptance Tests set out in clauses 9.5 or 9.6, as the case may be.

9.10 **Continued Acceptance Tests:** The process set out in clauses 9.8 and 9.9 may, at the request of Police, be repeated, until the Acceptance Tests demonstrate to the satisfaction of Police (acting reasonably) that the Acceptance Criteria for the relevant Deliverable have been met.

9.11 **Acceptance Testing failure:** Without limiting Police's other rights and remedies, if any repeat Acceptance Tests under clause 9.9 do not demonstrate to the satisfaction of Police (acting reasonably) that the Acceptance Criteria for any Deliverable have been met, Police may, by written notice to the Service Provider:

(a) require the Service Provider to undertake remedial work in accordance with clause 9.8; or

(b) reject the Deliverable and terminate this Agreement or the individual Statement of Work in accordance with clause 17.4(c).

9.12 **General:** Use of any Deliverable by Police does not constitute deemed, conditional or any other form of acceptance of that Deliverable. For the avoidance of doubt Police will not use any Deliverable in a production environment until a signed Acceptance Certificate has been issued. The issue by Police of any Acceptance Certificate (or any other form of sign-off) will

not release the Service Provider from its obligations under this Agreement, including the warranties set out in clause 13.

10. NEW RELEASES

10.1 **Notification of New Releases:** The Service Provider will immediately notify Police of any New Releases which will be, or have become, available relating to the Software. The Service Provider's notification of any New Releases pursuant to this clause 10.1 will include advising Police (at no additional cost) as to the extent that the installation of the relevant New Release will affect any part of Police's information technology or telecommunications' systems, including any likely functionality or performance consequences.

10.2 **Police's right to obtain New Releases:** Police may, at any time after receiving notification under clause 10.1, elect to obtain a New Release notified by the Service Provider. Police will be entitled to rely on the Service Provider's advice in deciding whether to obtain any New Release.

10.3 **Supply of New Releases:** Where Police elects to obtain any New Release under clause 10.2, the Service Provider will (at its own cost) promptly supply the New Release to Police and, unless otherwise agreed, provide the following services, if requested by Police:

(a) installation and testing of the New Release;

(b) training of Police on a Train the Trainer basis in Auckland, Wellington or Christchurch to allow it to fully utilise the New Release; and

(c) provision of any updated Documentation incorporating information on the New Release, such as user manuals, systems manuals and training manuals.

10.4 **Right to refuse New Releases:** Police will be under no obligation to obtain any New Release notified by the Service Provider pursuant to clause 10.1. Refusal by Police to obtain any New Release will not affect its entitlement to the Services under this Agreement

10.5 **New Releases not to detrimentally affect the Software:** The Service Provider will ensure that each New Release supplied by the Service Provider pursuant to this Agreement does not cause any disruption or have any adverse impact on the Software (or any part of it) except in the manner and to the extent specifically and clearly described in writing by the Service Provider and accepted by Police prior to the supply of the New Release.

11. FEES AND PAYMENT

11.1 **Fees:** Police will pay the Fees and GST (if any) to the Service Provider in consideration of the Services and Deliverables.

11.2 **No other amounts payable:** The Service Provider:

(a) acknowledges that, except as expressly specified in this Agreement, no other payments or benefits will be payable or provided by Police to the Service Provider, including in relation to any of the Personnel; and

(b) indemnifies Police from and against any and all liability, losses, damages, costs and expenses awarded against, incurred or suffered by Police arising out of any failure to pay compensation, taxes, duties, levies or benefits in respect of any Personnel.

11.3 **Invoices:** The Service Provider will issue Police with invoices for the Fees on the dates or at the times specified in the relevant Statement of Work. Each invoice must be:

(a) a valid tax invoice for the purposes of the GST Act; and

(b) accompanied by such information reasonably requested by Police from time to time to support the Services and Deliverables being invoiced, (**Valid Tax Invoice**).

11.4 **Date for Payment:** Subject to clause 11.5, Police will make payment in respect of each Valid Tax Invoice by the 20th day of the month following the month in which the Valid Tax Invoice was received by Police.

11.5 **Dispute over invoice:** 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.

11.6 **Payment terms:** All sums due to the Service Provider under this Agreement:

(a) are exclusive of any GST which, where applicable, will be payable by Police to the Service Provider in addition to the Fees stated; and

(b) will be paid to the credit of a bank account to be designated in writing by the Service Provider.

11.7 **Expenses:**

(a) The Service Provider is responsible for all expenses incurred by it under this Agreement, unless otherwise expressly specified in the relevant Statement of Work.

(b) If the relevant Statement of Work specifies that Police is to reimburse the Service Provider for any particular expenses incurred by the Service Provider, then the Service Provider must:

(i) produce receipts or other reasonable evidence of such expenses on request;

(ii) provide a Valid Tax Invoice for the expenses; and

(iii) follow all of Police's expense guidelines and policies notified to the Service Provider from time to time when incurring the expenses.

11.8 **Set off:** Police may set-off any refund or other amount owing to Police from the Service Provider against any amount payable by Police under this Agreement.

11.9 **Benchmarking:**

(a) After expiry of 1 year from the Commencement Date of the relevant Statement of Work, Police may from time to time (but not more than once in any 12 month period) by notice to Service Provider conduct benchmarking exercises in respect of the Fees under that Statement of Work in accordance with Schedule 5 ("benchmarking").

(b) If the benchmarker determines in accordance with Schedule 5 that the Fees under the relevant Statement of Work do not fall within the lower quartile of prices for Comparable Fees (as defined in Schedule 10), Service Provider must within 20 Business Days of the benchmarker's report reduce the Fees to ensure that the Fees fall within the lower quartile.

12. DOCUMENTATION, RECORDS AND AUDIT

12.1 **Documentation:** The Service Provider will supply Police with the Documentation in accordance with the requirements set out in each Statement of Work.

12.2 **Records:** Without limiting its other obligations under this Agreement or at law, the Service Provider must create and maintain, and must ensure that each subcontractor creates and maintains, full, accurate and accessible Records relating to the provision of the Services and Deliverables and the Fees charged under this Agreement, to the standards required under the Public Records Act 2005, as notified by Police from time to time.

12.3 **Content of Records:** Without limiting clause 12.2:

(a) the Records created and maintained under clause 12.2 must, at a minimum, describe or specify:

(i) the nature and scope of the Services and Deliverables provided under this Agreement;

(ii) the transactions that took place in the provision of all Services and Deliverables;

(iii) the basis on which each invoice has been prepared and submitted to Police under this Agreement; and

(iv) any other information reasonably required by Police from time to time; and

(b) the Service Provider must ensure the Records created and maintained under clause 12.2 are:

(i) maintained in an accessible form;

(ii) retained for the Term; and

(iii) provided to Police in an accessible form on termination or expiry of this Agreement or the relevant Statement of Work and at any other time on Police's request.

12.4 **Audit:** Police may at any time notify the Service Provider that Police wishes to audit any or all of the Service Provider's:

(a) provision of the Services and Deliverables;

(b) invoicing; and

(c) compliance with the terms of this Agreement,

provided that Police may only conduct an audit once in any 12 month period and at any other time where Police has reasonable grounds to suspect the Service Provider has not complied with this Agreement.

12.5 **Notice of audit:** Police will notify the Service Provider of the date on which the audit will commence, which must be at least two Business Days after receipt of a notice under clause 12.4. The Service Provider will allow Police or its independent nominee to inspect the Service Provider's premises, systems used in the delivery of the Services and Deliverables and records on and from the date notified by Police during the Service Provider's normal business hours for the purpose of conducting the audit. Police will comply with the Service Provider's reasonable security and confidentiality requirements in conducting any audit under this clause 12.5.

12.6 **Assistance:** The Service Provider will assist Police with any audit conducted under clause 12.5 and will ensure its Personnel and subcontractors also assist Police, including by making their premises, systems used in the delivery of the Services and Deliverables and records available to Police or its independent nominee if requested.

12.7 **Costs:** Police will meet its costs of any audit unless the audit discloses that the Service Provider has overcharged Police on any invoice by 5% or more. In that case, the Service Provider will meet Police's audit costs.

12.8 **Non-compliance:** Without limiting any of Police's other rights or remedies, if any audit conducted under clause 12.5 discloses any failure to comply with this Agreement by the Service Provider, the Service Provider will promptly remedy the non-compliance. The Service Provider will refund any amounts overcharged by the Service Provider within five Business Days of completion of an audit and delivery of an audit report.

12.9 **OIA:** The Service Provider acknowledges that Police is subject to the OIA. The Service Provider agrees to cooperate fully in providing Police with any documents or other information that Police is required to provide pursuant to a request made under the OIA, or pursuant to questions raised in Parliament or in any Select Committee concerning this Agreement.

13. WARRANTIES

13.1 **Warranties:** The Service Provider warrants at all times that:

(a) all information supplied by it to Police under this Agreement is true, complete and accurate;

(b) it has full corporate power and has obtained the required authority and authorisations to enter into and perform its obligations under this Agreement;

(c) the Services and Deliverables will be provided in a timely manner and to a high standard of skill, care and diligence;

(d) it will comply with all timeframes and milestones set out in the relevant Statement of Work or otherwise agreed in writing by the parties;

(e) the Services and Deliverables comply with their relevant Specifications in all respects;

(f) the Deliverables and the Services meet, and represent an appropriate solution to, the Police Requirements;

(g) all Deliverables are fully compatible with, and integrate and operate satisfactorily in conjunction with, the other Deliverables and with Police's information technology and telecommunications systems as specified in the Statement of Work;

(h) all Services and Deliverables, and all software recommended by the Service Provider in connection with this Agreement, meets, and represents an appropriate solution to, the Police Requirements as specified in the Statement of Work;

(i) no Deliverable contains any known computer viruses, interruptions, logic bombs, Trojan horses or other forms of malicious code or performance impediments;

(j) all advice, including advice regarding hardware sizing, technical architecture and service levels, provided by the Service Provider in connection with this Agreement is provided to a high standard of skill, care and diligence, and to a level reflective of, and in accordance with, a high level of industry knowledge and competence; and

(k) all Documentation provided by the Service Provider under or in connection with this Agreement will:

(i) contain sufficient information for the full and efficient operation of the relevant Deliverables and Services to which the Documentation relates in the manner contemplated by Police;

(ii) correctly represent the attributes of the subject matter to which it relates;

(iii) provide proper and adequate instructions for its intended purpose; and

(iv) be written or delivered in language and at a level appropriate for the intended audience.

13.2 **System warranties:** The System will, for so long as support services are to be provided by the Service Provider in respect of the System:

(a) meet and satisfy the Specifications;

(b) be fit for the purpose for such System as specified in the applicable Statement(s) of Work; and

(c) be free from bugs, viruses and material defects and errors.

The Service Provider shall not be liable for breach of this clause 13.2 to the extent that the breach arises as a direct result of any part of the System not supplied by the Service Provider not performing in accordance with its applicable specifications in any material respect.

13.3 **Remedies for failure:** If the Service Provider breaches any warranty set out in clauses 13.1(c) to (k) or 13.2, then, without limiting Police's other rights or remedies:

(a) the Service Provider must promptly remedy the breach at its cost upon receipt of notice in writing from Police requiring the breach to be remedied within 20 business days;

(b) if the Service Provider fails to remedy the breach to Police's reasonable satisfaction within the time specified in Police's notice given under clause 13.2(a), Police may, without limiting its other rights and remedies:

(i) withhold payment of any invoices directly relating to the breach due to the Service Provider until the matter is resolved to Police's reasonable satisfaction; or

(ii) remedy the defect itself, or by contracting a third party to do so, at the Service Provider's cost.

13.4 **Third party warranties:** The Service Provider will assign to Police, or if it is unable to do so, will hold for the sole benefit of Police, all warranties and guarantees provided by third parties to the Service Provider in respect of the provision of any Services and Deliverables under this Agreement.

13.5 **Warranties additional:** The express warranties provided by the Service Provider under this Agreement are additional to any other warranties or guarantees given by the Service Provider or implied by custom or law.

14. INDEMNITY, LIABILITY AND INSURANCE

14.1 **Indemnity:** Subject to clause 14.2, the Service Provider will at all times indemnify Police and Police's officers, employees and agents from and against all liability, losses, damages, costs and expenses of any nature whatsoever awarded against, incurred or suffered by them, directly arising out of or resulting from:

(a) the non-performance or breach by the Service Provider of any of its obligations under this Agreement; or

(b) the negligence of the Service Provider or its Personnel or subcontractors.

14.2 **Service Provider's liability:** Subject to clauses 14.4 and 14.5, the Service Provider's total aggregate liability under or in connection with this Agreement, whether in contract or tort (including negligence) or otherwise, is limited to an amount equal to the greater of:

(a) One times the Fees paid and the Fees payable under the relevant Statement of Work in respect of Equipment plus three times the Fees paid and the Fees payable under the relevant Statement of Work in respect of Services; and

(b) the amount set out in Schedule 1.

14.3 **Police's liability:** Subject to clauses 14.4 and 14.5, Police's total aggregate liability under or in connection with this Agreement, whether in contract or tort (including negligence) or otherwise, is limited to an amount equal to the Fees paid and the Fees payable under the relevant Statement of Work.

14.4 Neither party will under any circumstances be liable in relation to this Agreement for any indirect or consequential loss or damage, including loss of profits, arising out of or in connection with the performance or non-performance of this Agreement

14.5 **Exclusions:** Nothing in clauses 14.2 to 14.4 limits or excludes:

(a) either party's liability under clause 15 in relation to IP Claims; or

(b) either party's liability for breach of clause 16: or

(c) the Service Provider's liability for any fraudulent, wilful, or unlawful act or omission; or

(d) the Service Provider's liability for damage to Police premises (including for damage caused by a contractor of the Service Provider). The Service Provider's liability for damage to Police premises shall, whether such liability arises in contract or tort (including negligence) or otherwise, be limited to NZ$50,000,000.

14.6 **Insurance:** During the Term and for three years after termination or expiry of this Agreement, the Service Provider will maintain insurance coverage in amounts and against risks that are normal for businesses similar to that of the Service Provider, and in particular will maintain coverage in respect of public liability, professional indemnity and property damage in the amounts set out in Schedule 1. The Service Provider will, upon request at any time, provide Police with a certificate from the insurer or insurers confirming the terms of such insurance.

15. INTELLECTUAL PROPERTY RIGHTS

15.1 **Ownership of existing IP:** Each party or its licensors retains ownership of all Intellectual Property Rights in Existing Material belonging to that party or its licensors. The Service Provider acknowledges and agrees that all Intellectual Property Rights in the Police Data will be owned by Police.

15.2 **Police owns new IP:** Subject to clause 15.1, all Intellectual Property Rights in all:

(a) Deliverables, including all Developed Software but excluding Proprietary Software;

(b) enhancements, modifications or adaptations to any Existing Material; and

(c) other materials,

developed, commissioned or created under or in connection with this Agreement, will immediately and directly vest in Police upon their creation. To the extent such ownership does not so vest, the Service Provider irrevocably assigns such Intellectual Property Rights to Police. The Service Provider will ensure all moral rights in such Intellectual Property Rights are waived before provision of the Deliverables to Police.

15.3 **Licence to Police:** Notwithstanding clause 15.1, the Service Provider grants Police (and its third party service providers engaged by Police in connection with Police's use of the Deliverables) a perpetual, non-exclusive, and irrevocable license to exercise for Police's statutory and operational purposes all Intellectual Property Rights in all Deliverables that are not owned by Police or otherwise licensed to Police under this Agreement. This licence includes the right to use, copy and modify such Deliverables. The licence to any third party service providers of Police under this clause is conditional on such providers signing confidentiality agreements no less stringent than the confidentiality obligations to which Police is subject under this Agreement. As part of the licence granted to Police under this Agreement, Police shall be entitled to permit Public Safety Organisations to use the System and the applicable Deliverables while such organisations share premises with Police.

15.4 **Licence to Service Provider:** Police grants the Service Provider a non-exclusive licence to exercise, only for the Term and to the extent necessary to provide the Services and Deliverables, all Intellectual Property Rights provided by or on behalf of Police under this Agreement.

15.5 **Title and risk:** The parties agree that title to, and risk in, any media on which any Deliverable is recorded, will pass to Police on delivery to Police, unless otherwise agreed in writing by the parties.

15.6 **Service Provider warranty:** The Service Provider represents and warrants that:

(a) it has full right and title to vest the applicable Intellectual Property Rights (excluding rights in the Proprietary Software) in Police in accordance with clause 15.2;

(b) it is authorised to licence Intellectual Property Rights to Police and its third party service providers in accordance with clause 15.3;

(c) the exercise in accordance with this Agreement of any Intellectual Property Right vested in or licensed to Police or any Related Party under this Agreement will not infringe the rights of any third party; and

(d) it has obtained and/or will make available to Police and its Related Parties all licenses, clearances, consents and authorisations necessary for the use of the Services and Deliverables in accordance with this Agreement.

15.7 **Intellectual Property Rights indemnity:**

(a) The Service Provider will fully indemnify Police against all liability, losses, damages, costs and expenses suffered or incurred by Police as a result of any claim or threatened claim alleging that any of the Deliverables or Services, or Police's or a Related Party's use or possession of any of them, infringes the Intellectual Property Rights of any person (**IP Claim**).

(b) Each party will promptly notify the other party in writing upon becoming aware of any IP Claim.

(c) Unless otherwise required by Police, the Service Provider will control the conduct of any IP Claim and all negotiations for its settlement or compromise but in all cases will:

(i) consult with Police and keep Police fully informed of such matters;

(ii) ensure that Police's name and business reputation are not adversely affected by any such steps taken.

(d) Police will co-operate with the Service Provider in defending or settling any IP Claim under this clause 15.7 and will endeavour to make its employees available to give statements, information and evidence as the Service Provider may reasonably request.

15.8 **Police remedies:** If any IP Claim prevents or threatens to prevent the supply or exploitation of a Service or Deliverable then the Service Provider must, at the request of and at no cost to Police or its third party service providers:

(a) obtain for Police and its third party service providers the right to continue the supply or exploitation;

(b) modify the Service or Deliverable so it becomes non-infringing; or

(c) replace the Deliverable with another non-infringing item,

provided that the Service Provider must ensure that the remedy does not materially affect the Service or Deliverable or Police's or its third party service providers' exploitation of it. Without prejudice to any right or remedy, Police may terminate this Agreement if the Service Provider is unable to remedy the IP Claim in accordance with this clause 15.8 within two months of Police's request.

15.9 **Source Materials:** The Service Provider must provide all Developed Software to Police in object code form and, unless otherwise specified in a Statement of Work, must also provide Police with the Source Materials for that Software at the same time.

15.10 **Escrow:** The Service Provider must:

(a) if and to the extent requested by Police in a Statement of Work, enter into an escrow agreement in relation to the Source Materials of any Developed Software (each such escrow agreement being an **Escrow Agreement**);

(b) ensure that such an Escrow Agreement is in a form, and entered into with an escrow agent, approved by Police and provides, among other things:

(i) for the deposit by the Service Provider of the Source Materials of the version of all such Software currently being used by Police; and

(ii) for the release of the Source Materials for the Software by the escrow agent to Police in the event that any of the release events described in the Escrow Agreement occurs or is threatened to occur.

(c) use reasonable commercial endeavours to assist Police to put in place source code escrow arrangements with the applicable third party licensors regarding Software that is not owned by the Service Provider.

16. CONFIDENTIAL INFORMATION

16.1 **Confidentiality obligations:** The Receiving Party must:

(a) use the Disclosing Party's Confidential Information solely for the purpose of, and solely to the extent necessary for, exercising the Receiving Party's rights and complying with the Receiving Party's obligations under this Agreement;

(b) only disclose the Disclosing Party's Confidential Information to those of the Receiving Party's employees, agents and contractors (and in Police's case, Public Safety Organisations) to whom, and to the extent that, such disclosure is reasonably necessary for the purpose of exercising the Receiving Party's rights and complying with the Receiving Party's obligations under this Agreement; and

(c) maintain effective and adequate security measures to:

(i) safeguard the Disclosing Party's Confidential Information from access or use by unauthorised persons; and

(ii) keep the Disclosing Party's Confidential Information under the Receiving Party's control,

such measures being to a high standard of care, and in any event being at least to the same standard of care used by the Receiving Party for its own Confidential Information.

16.2 **Exceptions to obligations:** The provisions of clause 16.1 will not apply to Confidential Information, to the extent that the Confidential Information:

(a) was, before the Receiving Party received such Confidential Information from the Disclosing Party, in the Receiving Party's possession without any obligations of confidence;

(b) is independently acquired or developed by the Receiving Party without breaching any of the Receiving Party's obligations under this Agreement and without use of any other Confidential Information of the Disclosing Party;

(c) is subsequently disclosed to the Receiving Party, without any obligations of confidence, by a third party who has not derived it, directly or indirectly, from the Disclosing Party;

(d) is or becomes generally available to the public through no act or default of the Receiving Party or any of the Receiving Party's employees, agents or subcontractors; or

(e) is required to be disclosed by law, or to the courts of any competent jurisdiction, or to any government regulatory or financial authority.

16.3 **Disclosure to Personnel:** The Service Provider must ensure that any person to whom the Service Provider makes any disclosure in accordance with clause 16.1(b):

(a) is made aware of, and subject to, the Service Provider's obligations under clause 16.1; and

(b) has entered into a written undertaking of confidentiality in favour of the Service Provider or, if requested by Police, in favour of Police, that is at least as restrictive as the undertakings set out in clause 16.1 and that applies to the Confidential Information,

and the Service Provider remains responsible to Police for any unauthorised use or disclosure of Police's Confidential Information by such persons as if the use or disclosure was made by the Service Provider under this clause 16.

16.4 **Misuse or breach:** The Service Provider will notify Police in writing immediately upon becoming aware of any:

(a) potential, threatened or actual misuse or unauthorised disclosure of Confidential Information by any person to whom the Service Provider makes any disclosure in accordance with clause 16.1(b); or

(b) breach of the Service Provider's obligations under this clause 16,

and will co-operate with Police in preventing or limiting such misuse, unauthorised disclosure or breach, at the cost of the Service Provider.

16.5 **Equitable relief:** Each party acknowledges that any breach of this clause 16 by the Receiving Party may cause the Disclosing Party irreparable harm for which damages would not be an adequate remedy. In addition to any other remedy available to it, the Disclosing Party may seek equitable relief (including injunctive relief or specific performance) against any breach or threatened breach of this clause 16 by the Receiving Party.

16.6 **No limitation:** Nothing in this clause limits or restricts any rights granted to Police under clause 15.

16.7 **Announcements:** The Service Provider must not make any announcement regarding this Agreement to any person, without Police's prior written consent.

16.8 **Export of Police Data:** The Service Provider must not:

(a) transfer any Police Data outside of New Zealand;

(b) make any Police Data available to any person outside of New Zealand; or

(c) permit or authorise any of the things described in (a) and (b) to occur, without first obtaining Police written consent.

17. TERM AND TERMINATION

17.1 **Commencement and initial term:** This Agreement will commence on the Commencement Date and, unless terminated earlier in accordance with its terms, will continue in full force and effect until the Expiry Date.

17.2 **Renewal:** This Agreement may be renewed by Police for the renewal period or periods set out in Schedule 1.

17.3 **Termination for convenience:** Police may terminate this Agreement or one or more Statements of Work at any time by giving the Service Provider at least 90 days' written notice. Provided that where Police elect to terminate this Agreement or a Statement of Work under this clause then Police will only pay the Service Provider's termination costs incurred in the provision of Services and Deliverables as specified in the Statement of Work.

17.4 **Termination for Service Provider's breach:** Without prejudice to any other right or remedy it may have, Police may immediately terminate this Agreement or one or more Statements of Work at any time by notice in writing to the Service Provider if:

(a) the Service Provider is in material breach of this Agreement or any Statement of Work and, in the case of a material breach capable of remedy, the material breach is not remedied within 20 Business Days of the Service Provider receiving written notice specifying the material breach and requiring its remedy;

(b) the Service Provider is in material breach of this Agreement or any Statement of Work and the material breach is not capable of remedy;

(c) any repeat Acceptance Tests undertaken under clause 9.9 do not demonstrate (to the satisfaction of Police) the Acceptance Criteria for any Deliverable have been met;

(d) the Service Provider ceases or threatens to cease to carry on all or substantially all of its business or operations;

(e) the Service Provider is declared or becomes bankrupt or insolvent, is unable to pay its debts as they fall due, enters into a general assignment of its indebtedness or a scheme of arrangement or composition with its creditors, or takes or suffers any similar or analogous action in consequence of debt; or

(f) the Service Provider has a trustee, manager, administrator, administrative receiver, receiver, inspector under legislation or similar officer appointed in respect of the whole or any part of the Service Provider's assets or business, or an order is made or a resolution is passed for the liquidation of the Service Provider.

17.5 **Termination for Police's breach:** Without prejudice to any other right or remedy it may have, the Service Provider may immediately terminate this Agreement at any time by giving to Police notice in writing if:

(a) Police fails to pay any Fees that are not the subject of a dispute between the parties under clause 11.5 by the due date and if:

(i) the failure to pay is not remedied within 20 Business Days of Police receiving written notice from the Service Provider specifying the failure to pay and requiring payment.

(b) Police is in material breach of this Agreement, other than a failure to pay any Fees, and the material breach is not remedied within 20 Business Days of Police receiving notice specifying the material breach, requiring its remedy and specifying failure to remedy may result in termination.

17.6 **Consequences of termination:** On termination or expiry of this Agreement or one or more Statements of Work for any reason:

(a) the Service Provider will, subject to clause 17.6(e), cease to provide the relevant Services and Deliverables;

(b) the Service Provider will return to Police all Police Property and other property that Police has provided to the Service Provider under or in connection with this Agreement or the relevant Statements of Work;

(c) the Service Provider will, upon receipt of a written request from Police:

(i) where this Agreement is terminated or expires in its entirety, return or destroy (at Police's option), all Confidential Information in the possession or control of the Service Provider or any Personnel or subcontractor; or

(ii) where one or more Statements of Work are terminated or expire, return or destroy (at Police's option), all Confidential Information in the possession or control of the Service Provider or any Personnel or subcontractor relating to those Statements of Work; and

upon the return or destruction (as the case may be) of such Confidential Information, the Service Provider will provide to Police a certificate stating that the Confidential Information returned or destroyed comprises all of the applicable Confidential Information in the possession or control of the Service Provider or any Personnel or subcontractor;

(d) the Service Provider will provide such information and assistance as Police requires to allow Police to make an orderly transition of all or any of the Services and Deliverables to Police and/or any nominated alternative service provider, including by using its reasonable endeavours to transfer to Police the benefit of all subcontracts that it has entered in to which relate to the applicable Services and Deliverables where requested to do so by Police; and

(e) the Service Provider will, for up to six months (or for such further period as may be agreed) after termination or expiry, continue to offer the applicable Services and Deliverables to Police, under the terms of this Agreement as Police may reasonably require while Police makes the transition to an alternative service provider, and during that six month period the Service Provider will charge Police at the rates set out in the Statement of Work for those Services and Deliverables unless otherwise agreed in writing.

17.7 **Survival of provisions:** Upon termination or expiry of this Agreement for any reason, the provisions of clauses 5.1(c), 11.2, 11.5 to 11.8, 12.2, 12.3, 13, 14, 15, 16.1 to 16.7, 16.10, 17.6 to 17.8 and 20 and any other clauses intended to survive termination or expiry, together with those other provisions of this Agreement that are required in order to give effect to those clauses, will remain in full force and effect.

17.8 **Accrued rights:** Termination or expiry of this Agreement will be without prejudice to the rights and remedies of the parties accrued prior to termination or expiry, including in respect of any prior breach of this Agreement.

17.9 **Step-in rights**

(a) Without prejudice to and in addition to any other rights Police may have under this Agreement or at law, and in particular the right under clause 17.4(a), if:

(i) The Service Provider commits a material breach of this Agreement; and

(ii) Police has given the Service Provider written notice requiring it to remedy the material breach within fifteen Business Days and at the end of that period the material breach is still unremedied; and

(iii) Police has given the Service Provider a further written notice advising the Service Provider that if at the end of a 24 hour period after receipt by the Service Provider of such notice the material breach remains unremedied, Police intends to use a third party to remedy such services, and if at the end of 24 hours after receipt by the Service Provider of such notice, such material breach remains unremedied,

Police may, at its option, take control of the relevant Deliverables and/or Services, and in doing so, may take such other action as is reasonably necessary to restore performance in accordance with this Agreement in relation to the affected Deliverables and/or Services, subject to the party requested by Police to provide services complying with the Service Provider's reasonable confidentiality, safety and security requirements.

(b) The Service Provider must co-operate fully with Police or its nominee and their agents and provide all reasonable assistance at no charge to restore performance in relation to the affected Deliverables and/or Services as soon as possible, including giving Police and its nominees reasonable access to the Service Provider's premises, equipment, software and materials that are used in the supply of the Deliverables and Services provided such nominee or agent shall enter into reasonable confidentiality obligations.

(c) Police shall cease any exercise of its rights under this clause 17.9 as soon as reasonably practicable after performance in accordance with this Agreement has been restored in relation to the affected Deliverables and/or Services but shall not be required to do so unless Police is reasonably satisfied that any identifiable root cause of the problem has been resolved.

(d) The Service Provider shall not be entitled to invoice Police for the Fees for that portion of the Deliverables and/or Services performed by Police or its agent under this clause.

(e) Nothing in this clause limits or increases the Service Provider's liability to Police with respect to any default or non-performance by the Service Provider under this Agreement.

(f) The Service Provider will not be responsible for any damage or defects caused by the other party requested by Police to provide services. Where the Service Provider is required to repair any such damage or defects the Service Provider may charge the reasonable cost of such repairs to Police.

18. DISPUTES

18.1 **Procedure:** Subject to clause 18.2, if a dispute arises in relation to this Agreement, the parties will attempt to resolve the dispute using the dispute resolution process set out below before pursuing any other remedies available at law or otherwise.

(a) If either party receives notice of a dispute, the parties will work together in good faith to resolve the dispute via negotiation and will escalate the dispute to appropriate levels within their respective organisations.

(b) If the dispute is not resolved within 20 Business Days of receipt of a notice under clause 18.1(a), then either party may, by written notice to the other party (**Mediation**

Notice), require the dispute to be submitted to mediation in New Zealand in accordance with the provisions of the then-current LEADR New Zealand Incorporated Standard Mediation Agreement (**Mediation**).

(c) The Mediation will be conducted by a mediator, and at a fee, agreed by the parties. If the parties fail to agree such matters within 10 Business Days following the date of the delivery of the Mediation Notice, the Chair for the time being of LEADR New Zealand Incorporated will select the mediator and determine the mediator's fee. The parties will share equally the cost of the mediator's fee.

18.2 **Interlocutory relief:** Nothing in this clause 18 will prevent either party, at any time, from seeking any urgent interlocutory relief from a court of competent jurisdiction in relation to any matter that arises under this Agreement.

18.3 **Other remedies:** Subject to clause 18.2, a party to the dispute will only be entitled to pursue other remedies available to it at law or otherwise, if the parties have failed to resolve the dispute within 20 Business Days after commencement of the Mediation.

18.4 **Continuity:** In the event of a dispute between the parties concerning this Agreement, the Service Provider will continue to provide the Services and Deliverables unless Police requires otherwise in writing.

19. FORCE MAJEURE

19.1 **Force Majeure Event:** Neither party will be liable to the other for any failure to perform any of its obligations under this Agreement to the extent the failure is caused by a Force Majeure Event, provided that the party seeking to rely on this clause 19.1 has:

(a) notified the other party as soon as practicable after the Force Majeure Event occurs and provided full information concerning the Force Majeure Event, including an estimate of the time likely to be required to overcome it;

(b) used its best endeavours to overcome the Force Majeure Event and minimise the loss to the other party; and

(c) continued to perform its obligations under this Agreement as far as practicable.

19.2 **Termination for Force Majeure Event:** If a Force Majeure Event prevents, or is likely to prevent, either party from complying with its obligations under this Agreement to a material extent for a continuous period of 20 Business Days or more, the other party may terminate this Agreement by giving the non-complying party at least 20 Business Days' notice in writing.

20. GENERAL

20.1 **Variations:** No amendment to this Agreement will be effective unless it is in writing and signed by the parties.

20.2 **Assignment:**

(a) The Service Provider may not assign, transfer, novate, subcontract, charge, pledge or otherwise encumber this Agreement, or any of its rights or obligations under this Agreement, without first obtaining Police's written consent.

(b) Any change in the Control of the Service Provider will be treated as an assignment by the Service Provider under clause 20.2(a).

(c) Police may, assign, transfer or novate any or all of its rights and obligations under this Agreement to any person, agency or regulatory body tasked by the Crown with fulfilling any of the functions of Police by giving notice in writing to the Service Provider.

20.3 **No waiver:**

(a) A delay, neglect or forbearance by a party in enforcing any provision of this Agreement against the other will not waive or limit any right of that party.

(b) No provision of this Agreement will be considered waived by a party unless that party waives the provision in writing.

(c) The parties will not treat a waiver by a party of any breach as a waiver of any continuing or re-occurring breach, unless the parties have expressly agreed to do so in writing.

20.4 **Invalid clauses:** If any part of this Agreement is held to be invalid, unenforceable or illegal for any reason, this Agreement will be deemed to be amended by the addition or deletion of wording necessary to remove the invalid, unenforceable or illegal part, but otherwise to retain the provisions of this Agreement to the maximum extent permissible under applicable law.

20.5 **Costs:** Each party will bear its own legal costs and expenses incurred in connection with the preparation, negotiation and execution of this Agreement.

20.6 **Relationship:**

(a) The parties will perform their obligations under this Agreement as independent contractors to each other.

(b) This Agreement will not create, constitute or evidence any partnership, joint venture, agency, trust or employer/employee relationship between the parties, unless it expressly states otherwise. Neither party may make or allow anyone to represent that any such relationship exists between the parties.

(c) Neither party will have the authority to act for, or incur any obligation on behalf of, the other party, except as expressly provided for in this Agreement.

20.7 **Entire agreement:** This Agreement contains the whole of the contract and understanding between the parties in respect of the matters covered by it and supersedes all prior representations, agreements, statements and understandings between the parties in respect of those matters, whether verbal or in writing.

20.8 **Remedies cumulative:** The rights of the parties under this Agreement are cumulative. The parties do not exclude any rights provided by law, unless otherwise expressly stated in this Agreement.

20.9 **Notices:** Each notice or other communication to be given under this Agreement (**Notice**) must be in writing and must be sent by post, facsimile (confirmed by post) or personal delivery to the addressee at the postal address, facsimile number or physical address, and marked for the attention of the person or office holder (if any), set out in Schedule 1. No Notice will be effective until received. A Notice is, however, deemed to be received:

(a) in the case of posting, on the third Business Day following the date of posting;

(b) in the case of personal delivery, when received; and

(c) in the case of a facsimile, following receipt of a report from the machine on which the facsimile was sent confirming that all pages were successfully transmitted,

provided that any Notice personally delivered or sent by facsimile either after 5pm on a Business Day or on any day that is not a Business Day will be deemed to have been received on the next Business Day.

20.10 **Governing Law:** This Agreement is governed by New Zealand law. Subject to clause 18, the parties submit to the non-exclusive jurisdiction of the New Zealand courts in respect of all matters relating to this Agreement.

20.11 **Counterparts:** This Agreement may be signed in any number of counterparts (including facsimile copies) all of which, when taken together, will constitute one and the same agreement. A party may enter into this Agreement by signing any counterpart.

20.12 **Further assurances:** Each party undertakes, at its own expense, to execute and deliver any document and to do all things as may reasonably be required in order to assist, in respect of matters within that party's control, the other party to obtain the full benefit of this Agreement according to its true intent, including assisting Police to register as proprietor of,

and to perfect Police's title to, any Intellectual Property Right owned by Police under this Agreement.

20.13 **Non merger:** The warranties, undertakings and indemnities given under this Agreement will not merge on any completion or settlement under this Agreement or any other agreement between the parties, but will remain enforceable to the fullest extent permissible, despite any rule of law to the contrary.

SIGNED

For **HER MAJESTY THE QUEEN IN RIGHT OF NEW ZEALAND** acting by and through the **COMMISSIONER OF POLICE** or his or her authorised delegate: Signature:	For [Legal Name of Service Provider]: Signature:
Name:	Name:
Position:	Position:
Date:	Date:

Witnessed by:	Witnessed by:
Name:	Name:
Date:	Date:

SCHEDULE 1: AGREEMENT DETAILS

The headings in this Schedule have legal effect.

Proposal (Clauses 1.1 and 2.4)	The Service Provider's proposal dated [xxxx] in response to Police's tender documentation advertised on [xxxxx] (Police reference number TN xxxx).	
SERVICE PROVIDER'S LIABILITY CAP (Clause 14.2(b))	$20 million	
INSURANCE REQUIREMENTS (Clause 14.5)	**Insurance type**	**Amount**
	Professional indemnity	$15 million
	Public liability	$15 million
	Property damage	$20 million
COMMENCEMENT DATE (Clause 17.1)	The date on which both parties to this Agreement have signed this Agreement.	
EXPIRY DATE (Clause 17.1)	xx years from the Commencement Date	
RENEWAL (Clause 17.2)	Police may extend the term of this Agreement for up to xxx periods of up to x years each by giving the Service Provider notice in writing at least 90 Business Days before the Expiry Date, or the expiry of the relevant renewal period, as the case may be.	
POLICE'S NOTICE DETAILS (Clause 20.9)	Address for Notices:	New Zealand Police, P O Box 3017, Wellington Police National Headquarters, 180 Molesworth Street, Thorndon, Wellington
	E-mail:	Steven.full@police.govt.nz
	Phone:	04 238 3336
	Attention:	Steven Full, Manager ICT Strategic Sourcing
SERVICE PROVIDER'S NOTICE DETAILS (Clause 20.9)	Address for Notices:	
	E-mail:	
	Phone	
	Attention:	

SCHEDULE 2: PROJECT STATEMENT OF WORK TEMPLATE

PROJECT NAME STATEMENT OF WORK

This Statement of Work records the terms on which certain deliverables and/or related support and maintenance services and/or professional services will be provided by **[X]** (**Service Provider**) to **HER MAJESTY THE QUEEN IN RIGHT OF NEW ZEALAND** acting by and through the **COMMISSIONER OF POLICE** or his or her duly authorised delegate (**Police**).

1. MASTER AGREEMENT

1.1 **Background:** [Insert brief background to the Services and Deliverables (refer to the relevant Police project or business unit) and to the Service Provider's role. The background should tell the reader instantly what this Statement of Work is all about. Summarise the Services and Deliverables in simple terms – the summary gives context and should be clear enough to a reader who doesn't know anything about the project or Services and Deliverables Police is purchasing.

Example:

The Service Provider will provide detailed design and software development services to Police to replace the existing X environment. Once implemented and accepted, the Service Provider will provide ongoing support and maintenance for the new X environment.]

1.2 **Subject to Master Agreement:** This Statement of Work is entered into under, and is governed by and subject to, the Master ICT Services Agreement dated [insert date] between the Service Provider and Police (**Master Agreement**).

1.3 **Interpretation:** Unless the context otherwise requires, terms defined in the Master Agreement bear the same meaning in this Statement of Work and the rules of interpretation recorded in clause 1 of the Master Agreement apply to this Statement of Work (except that references to paragraphs and appendices in this Statement of Work are references to the paragraphs and appendices of this Statement of Work).

2. TERM

2.1 **Term:** This Statement of Work will commence on [***insert date***] (**Statement of Work Start Date**) and, unless otherwise terminated or removed in accordance with the provisions of the Master Agreement, will continue until Police notifies the Service Provider in writing that the Service Provider has completed the supply of the Deliverables and/or the performance of the Services in accordance with this Statement of Work to the satisfaction of Police (**Statement of Work Term**).

2.2 **Consistent with Term of Master Agreement:** Notwithstanding any other provision of this Statement of Work, this Statement of Work will terminate immediately upon the termination of the Master Agreement.

[Notes for paragrah 3.1 (Services) and paragraph 3.2 (Deliverables) - Insert a detailed description of the Services and the Deliverables to be provided. This Services and Deliverables section is one of the most important parts of this Agreement – the provisions here tell the reader what Services and Deliverables Police is purchasing.]

3. SERVICES

3.1 **Services:** The Services that the Service Provider will provide to Police include:

Use subparagraphs to set out each task if necessary.

Example:

(a) preparing a high level design of the X solution containing the following detail:

(i) [insert detail]; and

(ii) [insert detail];

(b) preparing a detailed design of the X solution based on the high level design containing the following detail:

(i) [insert detail]; and

(ii) [insert detail];

(c) supplying all component parts of the agreed X solution, writing all required software, integrating the components, testing the solution and implementing the solution in a go live environment.]

[OR Breakdown into different service streams with headings if required, and then insert more detail under each heading.

Example:

(a) Detailed Design Services

[Insert detail of the detailed design work services]

(b) Software Development Services

[Insert detail of the software development services to be provided based on the detailed design]

[OR Consider including a table that sets out services that are in scope and those that are out of scope for clarity.

Example:

Services – in scope	Services – out of scope
High level and detailed design documents Supply of Developed Software Supply of Proprietary Software	Data migration Supply of Equipment Management of physical environment including servers

3.2 **Service Levels:** The Service Provider will meet or exceed the following Service Levels:

[Using Example 1 in paragraph 3.1 above:

(a) produce and provide the high level design by 31 July 2008;

(b) prepare a detailed design of the X solution based on the high level design by 30 September 2008; and

(c) develop and deliver the solution, test the solution and implement the solution in a go live environment by 31 October 2008.]

4. DELIVERABLES

4.1 **Deliverables:** The Service Provider will provide to Police the Software (if any) described in paragraphs 4.2 and 4.4 and the following other Deliverables:

[Use subparagraphs to set out each deliverable if necessary.

Example:

(a) high level design document described in paragraph 3.1(a);

(b) detailed design document described in paragraph 3.1(b); and

(c) all other Deliverables required to deliver the overall solution to Police in accordance with this Statement of Work.]

4.2 **Developed Software:** The Developed Software comprises:

[Insert list of Developed Software. Use subparagraphs beginning with (a)…]

[OR Insert "Not applicable" if there is no Developed Software.]

4.3 **Specifications for Developed Software:** The specifications for the Developed Software are:

[Insert a detailed description of the business purposes and/or uses for which Police is obtaining the Developed Software and the functions that it is to perform.

Where appropriate, include cross references to documentation that the parties have agreed to that provide more detailed specifications.

Example:

(a) The Service Provider's Specifications dated 3 September 2008, entitled "X Solution for the Police – New X Environment (Specification Reference 0221116)"; and ....]

4.4 **Proprietary Software:** The Proprietary Software comprises:

[Insert list of Proprietary Software. Use subparagraphs beginning with (a)...]

[OR Insert "Not applicable" if there is no Proprietary Software.]

4.5 **Specifications for Proprietary Software:** The specifications for the Proprietary Software are:

[Insert a detailed description of the business purposes and/or uses for which Police is obtaining the Proprietary Software and the functions that it is to perform.

Where appropriate, include cross references to documentation that the parties have agreed to that provide more detailed specifications.

Example:

(a) The Service Provider's Specifications dated 5 September 2008, entitled "XXX Software (Manufacturer Number 222111)"; and ....]

4.6 **Other Deliverables:** The other Deliverables to be supplied by the Service Provider comprise:

[Insert list of other Deliverables. Use subparagraphs beginning with (a)...]

[OR Insert "Not applicable" if there are no other Deliverables.]

[Note that the Master Agreement does not contain specific terms dealing with the purchase of hardware. If hardware is being acquired under this Master Agreement, ICT Strategic Sourcing will need to review the Master Agreement and propose additional wording to deal with issues such as when title passes, PPSR issues, specific hardware warranty and support issues.]

4.7 **Specifications for Other Deliverables:** The specifications for the Deliverables other than the Developed Software and the Proprietary Software are:

[Insert a detailed description of the business purposes and/or uses for which Police is obtaining the Deliverables and the functions that they are to perform.

Where appropriate, include cross references to documentation that the parties have agreed to that provide more detailed specifications.]

5. DOCUMENTATION

The Service Provider will supply the following Documentation to Police:

[Insert a detailed description of the Documentation to be supplied by the Service Provider and any related requirements.]

6. ACCEPTANCE CRITERIA AND ACCEPTANCE TESTING

6.1 **Acceptance Criteria:** The Acceptance Criteria for the Deliverables are as follows:

[**Notes:** It is very important to complete this clause 6.1 where acceptance of a Deliverable (particularly Software) is subject to acceptance testing. Clause 9 of the Master Agreement sets out the general process for acceptance testing. This clause 6.1 sets out the specific criteria for which acceptance testing will be based on.]

Deliverables	Acceptance Criteria
[List each Deliverable listed in clause 15 (e.g. Developed Software, Proprietary	[Insert the acceptance criteria that applies to the Deliverable]

Deliverables	Acceptance Criteria
Software)]	

6.2 **Acceptance Test Plan:** All Software to be provided by the Service Provider under this Statement of Work must pass regression and integration testing undertaken in accordance with an Acceptance Test Plan detailed below or otherwise agreed in accordance with clause 9 of the Master Agreement:

[Insert details of the Acceptance Test Plan and other details relating to acceptance testing.]

7. PROJECT MANAGEMENT AND PERSONNEL

7.1 **Project Plan:** The Project Plan for this Statement of Work is recorded in appendix 1 to this Statement of Work.

7.2 **Specified Personnel:** The Specified Personnel and their respective functions are:

Specified Personnel	Component of Deliverables/Services for which Specified Personnel is responsible
[Insert name]	[Insert details]
[Insert name]	[Insert details]

8. MEETINGS AND REPORTING REQUIREMENTS

8.1 **Meeting Requirements:** The Service Provider's designated representatives will attend the following meetings at the following times:

Meeting Details	Designated representatives of the Service Provider required to attend	Frequency/Date
[Insert meeting details]	[Insert designated representatives]	[Insert date/frequency]
[Insert meeting details]	[Insert designated representatives]	[Insert date/frequency]

8.2 **Reporting Requirements:** The Service Provider will provide to Police the following reports at the following times:

Report Details	Frequency/Date
[Insert details of reports]	[Insert date/frequency]
[Insert details of reports]	[Insert date/frequency]

9. FEES

9.1 **Invoicing:** The Service Provider is to invoice the Fees:

[Choose one option for invoicing, insert relevant wording and delete remainder. Make sure all Fees are captured including both implementation and ongoing fees. Also, make sure you are clear on when invoicing commences. In particular, invoicing for ongoing support may not commence until expiry of a warranty period.]

On completion of the Services and supply of the Deliverables to Police's satisfaction.

OR

At the end of each month for Services and Deliverables provided during that month to Police's satisfaction.

OR [for fixed Fees]

In instalments on the dates set out below, subject to completion of the relevant milestones to Police's satisfaction:

Instalment (excluding GST)	Date	Milestone
[Insert amount of instalment] $	[Insert date of invoice]	[Describe Services or Deliverables to be provided before invoice is issued. Alternatively, Milestone payments may be tied to Deliverables meeting the Acceptance Criteria and passing their relevant Acceptance Tests.]

9.2 **Fees:**

[Specify the fees payable and the method and timing of invoices, including if any fees are only payable after acceptance of completion of milestones.]

[Choose one option, insert $ amount and delete remainder.]

Fixed Fee of $X excluding GST.

OR

[Use all or a percentage of the budgeted amount figure for the services as the maximum Fee. Specifying the maximum Fee protects Police from overspending the budgeted amount.]

Hourly Rate of $X excluding GST, up to a maximum Fee of $X excluding GST.

OR

Daily Rate of $X excluding GST, for each full day's attendances of 8 or more hours, reduced pro rata for attendance of less than 8 hours, up to a total maximum Fee of $X excluding GST.

OR

[Hourly/Daily Rates] for each of the Service Provider's Personnel in accordance with the following table of rates up to a maximum of $X excluding GST:

Personnel	[Hourly/Daily Rate] (excluding GST)
[Insert name of Personnel]	[Insert either hourly or daily rate as applicable]

9.3 **Expenses:**

[Choose one option, delete remainder.]

No reimbursement of expenses.

OR

Reimbursement for reasonable third party expenses incurred in the provision of the Services and Deliverables provided that:

(a) Police has given its prior written consent to the Service Provider incurring the expenses; and

(b) the expenses are charged at cost.

OR

Reimbursement of the following expenses to the limits set out in respect of each matter:

(a) Accommodation - $X

(b) Airfares - $X

(c) [Itemise other expenses] - $X.

Police is under no obligation to pay for any expense item once the specified expense limit for that item is exceeded.

OR

Reimbursement for reasonable third party expenses incurred in the provision of the Services and Deliverables up to a total of $X provided that Police is under no obligation to pay for any expense item once the total limit for expenses is exceeded.

10. VARIATIONS TO MASTER AGREEMENT [Delete this paragraph 10 if not applicable]

The terms and conditions of the Master Agreement will apply to this Statement of Work subject to the following variations for the purposes of this Statement of Work only:

[Insert description of any variation to the terms and conditions of the Master Agreement that apply in respect of this Statement of Work. Ensure that you consult with Corporate Legal before you vary any terms and conditions to the Master Agreement.]

11. OTHER TERMS [Delete this paragraph 11 if not applicable]

[Insert any additional terms that are to apply to the Statement of Work. Consider whether there are any additional risks to take into account. Ensure that you consult with Corporate Legal before you add any other terms and conditions to the Master Agreement.]

SIGNED:

For **HER MAJESTY THE QUEEN IN RIGHT OF NEW ZEALAND** acting by and through the **COMMISSIONER OF POLICE** or his or her authorised delegate:
Signature:
Name: [Insert Person with Financial Delegation]
Position:
Date:

For **[NAME OF SERVICE PROVIDER]**:
Signature:
Name:
Position:
Date:

Witnessed by:
Name:
Date:

Witnessed by:
Name:
Date:

APPENDIX 1

PROJECT PLAN

[Insert project plan or list of key Milestones and Milestone Dates.]

SCHEDULE 3: CHANGE CONTROL PROCESS

1. **Change Control Process**: The parties will follow the change control process described in this schedule 3 to initiate and consider:

   (a) new deliverables or services that are not within the scope of a Statement of Work; or

   (b) changes to the Deliverables or the Services (including any changes to the nature or scope of the Deliverables or the Services or to the timing or the delivery of the Deliverables or the Services) which cannot be accommodated by another process in this agreement, each being referred to in this agreement as a "Change".

2. **Change Request:** If either party wants to initiate a change that party will describe the details of the change in a written request to the other party **(Change Request).**

3. **Impact Report:** The service provider will, at its cost, prepare an impact report **(Impact Report)** detailing an explanation of the change, including how the change is to be implemented and, to the extent relevant, detailing:

   (a) the feasibility of the Change;

   (b) the effect of the Change on the ability of the Service Provider to meet its obligations under this agreement;

   (c) any cost implication for either party in relation to the Change;

   (d) any consequential material impacts of the Change;

   (e) where appropriate, suggested acceptance testing procedures and acceptance criteria for the proposed Change; and

   (f) such other information which is likely to be material to Police.

4. **Notify:** Police will, within a reasonable period of time from receipt of the relevant Impact Report, notify the service provider of its decision in respect of a change request including, without limitation, whether it:

   (a) accepts the Change Request;

   (b) wishes to renegotiate any aspect of the Change Request;

   (c) withdraws the Change Request, if initiated by Police; or

   (d) does not accept the Change Request, if initiated by the Service Provider.

5. **Pricing:** The following pricing principles will apply in respect of any change:

   (a) the Service Provider will only charge Police for a Change to the extent the Change cannot reasonably be considered already within the scope of this agreement (including within the scope of any Statement of Work);

   (b) if there is a cost impact of the Change then the parties will use genuine efforts to agree a reasonable price for the Change (taking into account the nature and extent of the Change) in accordance with the rest of this paragraph 5;

   (c) the pricing for any Change will be:

      i. reasonable;
      ii. competitive;
      iii. no higher than pricing the Service Provider offers its most preferred customers for products or services the same or similar to the products or services proposed to be provided to Police as part of the Change; and
      iv. no higher than the price at which Police would be able to procure similar products or services from another service provider; and

   (d) if requested by Police, the Service Provider will obtain and provide a certificate from an auditor confirming that any pricing of a Change complies with the requirements of this paragraph 5.

6. **Not Unreasonably Refuse Change:** The Service Provider must not unreasonably refuse (directly or indirectly) any change submitted by Police. Unreasonable grounds for refusing to provide a Change include, without limitation:

   (a) demanding unreasonable charges for the Change;

   (b) imposing unreasonable conditions for undertaking the Change; or

   (c) refusing to include the Change under this Agreement despite the subject matter of the Change being reasonably related to or connected with the Deliverables or the Services as they are at the relevant time.

7. **Agreement required:** The Service Provider will not undertake any Change unless Police and the Service Provider agree the details of the Change in writing in accordance with this Schedule 3 (which agreement will not be unreasonably withheld, in the case of the Service Provider). Any agreed Change will be formalised by the parties as an express variation to this Agreement.

8. **No obligation:** Police will not be bound to accept or pay for any unauthorised variations or changes to this Agreement or the Deliverables or the scope of the Services carried out by the Service Provider.

9. **Truncated Process:** Where:

   (a) the Change requested is relatively minor (in terms of cost and impact) and is fairly routine; or

   (b) if agreed by the parties (agreement not to be unreasonably withheld),

   a truncated Change Control Process (acceptable to Police) may be adopted to deal with any particular Change Request.

SCHEDULE 4: ACCEPTANCE CERTIFICATE

[Set out below is the template Acceptance Certificate to be completed by Police to demonstrate its satisfaction (acting reasonably) with a Deliverable as required under clause 9.7 of the Master Agreement.]

[Insert full name of Service Provider] (**Service Provider**) and **HER MAJESTY THE QUEEN IN RIGHT OF NEW ZEALAND** acting by and through the **COMMISSIONER OF POLICE** or his or her duly authorised delegate (**Police**) are parties to a Master ICT Services and Deliverables Agreement dated [insert date of Master Agreement] (**Master Agreement**) under which they entered into a Statement of Work requiring the Service Provider, among other things, to deliver [set out description of Deliverable. Include as an appendix where required] (**Deliverable**).

Without limiting Police's other rights and remedies, and the Service Provider's obligations, under the Master Agreement or otherwise, Police confirms that, on the basis of the Acceptance Testing undertaken, Police is satisfied that the Deliverable meets the Acceptance Criteria for that Deliverable in accordance with and for the purpose of clause 9.7 of the Master Agreement.

SIGNED

For and on behalf of **HER MAJESTY THE QUEEN IN RIGHT OF NEW ZEALAND** acting by and through the **COMMISSIONER OF POLICE** or his or her duly authorised delegate:

_____

[INSERT NAME]

In the presence of:

Witness Signature: _____

Witness Name: _____

Witness Occupation: _____

Witness Address: _____

SCHEDULE 5: BENCHMARKING

1. **Appointment of benchmarker**: The benchmarker will be appointed by agreement between the parties or, failing agreement within 10 Business Days of the date of Police's notice under clause 11.9, by the President of the New Zealand Institute of Chartered Accountants (or his/her nominee) on request by Police.

2. **Comparison:**
   (a) The benchmarking will compare the Fees against the charges for deliverables and services performed by other organisations which are comparable to the Deliverables and Services ("Comparable Products").

   (b) In order for deliverables or services to qualify as Comparable Products those deliverables and services must be sufficiently similar to the Deliverables and Services that the relevant data about those deliverables and services can meaningfully be normalised under paragraph 2(c) of this Schedule in order to be used as a comparator in the benchmarking.

   (c) For the purposes of the comparison the benchmarker must first normalise the charges for the Comparable Products by adjusting for differences that impede a like-for-like comparison, which may include differences in:

      (i) the scope, volume or complexity of the Comparable Products;

      (ii) the terms on which they are provided,

   but disregarding a difference in technology which reduces costs, such as the use of kiosks, where a provider of Comparable Products has adopted such technology but Service Provider has not.

3. **Cooperation:** The parties will co-operate with the benchmarker including promptly providing the benchmarker with:

   (a) all information and records relevant to the benchmarking requested by the benchmarker (including information and records relating to costs or profits); and

   (b) any access to facilities, systems or personnel reasonably required by the benchmarker in order to carry out the benchmarking.

4. **Review of initial findings:** Prior to issuing a final report the benchmarker will review the draft report with the parties. Both parties may within a reasonable period set by the benchmarker make submissions to the benchmarker as to the factual accuracy or completeness of the benchmark. The benchmarker will review the parties' submissions before issuing the final report in accordance with clause 5 of this schedule.

5. **Report:** The benchmarker will be required to deliver to each party within 40 Business Days of the commencement of the benchmarking (or such longer period as reasonably required by the benchmarker) a report which:

   (a) specifies the range of prices for Comparable Products (after adjustment under paragraph 2(c) of this Schedule) and where in the range the Fees fall; and

   (b) recommends any change to the Issuance Support Charge which, in the benchmarker's opinion, is necessary to ensure the Issuance Support Charge falls within the lower quartile of prices for Comparable Products (after adjustment under paragraph 2(c) of this Schedule), without recommending any change greater than necessary to do so.

6. **Confidential information and instruction:**
   (a) The benchmarker will not be required to disclose to either party any confidential information of third parties used by the benchmarker in preparing its report.

   (b) The benchmarker will be contracted and instructed by both parties to observe the requirements of this Schedule. If the benchmarker objects to any such requirement, the parties will act reasonably and in good faith to resolve the issue.

(c) The benchmarker must sign a tripartite confidentiality agreement with both parties, acceptable to both parties (acting reasonably), to protect both parties' confidential information.

(d) If the benchmarker attends a site of a party, the benchmarker must agree to comply with all reasonable security and health and safety obligations set by that party.

7. **Fees and costs:** Police will pay the benchmarker's fees for the benchmarking unless the benchmarker determines that Service Provider's pricing is not market competitive in which case Service Provider shall pay the benchmarker's fees. Each party will bear its own costs in connection with the benchmarking.

[**Notes:** The terms set out in this Schedule are a starting point for finalising the description of support and maintenance services and should be modified as required to suit the solution.

The Service Provider may have its own support and maintenance terms which, if acceptable to Police, can be substituted for the words set out below.

Delete this Schedule 6 if support and maintenance services are not required.]

SCHEDULE 6: SUPPORT AND MAINTENANCE SERVICES

1. SERVICES

1.1 Introduction/Overview

This Schedule describes the Support and Maintenance Services to be provided by the Service Provider to Police.

1.2 Service Summary

The Service Provider is responsible for the support and maintenance of Police's xxxx.

This includes, but is not limited to:

- Operating systems, middleware, infrastructure applications and tools.
- Maintenance and repair of Server Devices.

In support of change the Service Provider will also:

- Provide innovative and strategic advice pertaining to the Support and Maintenance Services (including that pertaining to database, information lifecycle, security, business continuity planning and infrastructure), which will assist in:
  - Optimising the xxxx Services;
  - Facilitating required change;
  - Improving return on investment.
- Review and accept planned change prior to release into production.
- Advise on changes in technology in the industry.
- Ensure documentation management and maintenance.

1.3 Subject to Master Agreement

This Schedule is entered into under, and is governed by and subject to, the Master ICT Services Agreement dated [insert date] between the Service Provider and Police (Master Agreement).

1.4 Term *(only leave this clause in if the Support Schedule is being added to an existing Master Agreement otherwise delete)*

This Schedule will commence on [insert date] (Schedule Start Date) and, unless otherwise terminated or removed in accordance with the provisions of the Master Agreement, will continue for the term of the Master Agreement.

Notwithstanding any other provision of this Schedule, this Schedule will terminate immediately upon the termination of the Master Agreement.

1.5 Interpretation

Unless the context otherwise requires, terms defined in the Master Agreement bear the same meaning in this Schedule and the rules of interpretation recorded in clause 1 of the Master Agreement apply to this Schedule (except that references to paragraphs and appendices in this Schedule are references to the paragraphs and appendices of this Schedule).

1.6 Glossary and Terms

Police is adopting ITIL (version 3) definitions for commonly employed ICT terminology. The listing below therefore excludes any term covered by ITIL which has no additional definition relating to the Police ICT Operating Environment.

This glossary is in addition to the terms specified in clause 1.1 of the Master ICT Services and Deliverables Agreement.

Term	Definition
Support and Maintenance Procedures	The procedures that apply to the Support and Maintenance Services as defined in the Procedures Manual.
Major Incident	Means the highest category of impact for an Incident classified as Priority 1 or Priority 2. A major Incident results in significant impact or disruption to Police.
Priority 1 or P1	Means Incidents classified as Priority 1 (P1) meaning: • Total failure of Service, for example: – Xxx applications not being available, or – All users not able to login to xxxx, or – ?? • Failure or degradation of xxx Services to multiple Police sites.
Priority 2 or P2	Means Incidents classified as Priority 2 (P2) meaning: • Partial failure or degradation of Service, for example: – a single Police site or user group not able to xxxx, or – ??? • Critical failures with an acceptable Workaround in place. • Failure or degradation of Service to a single Police site.
Priority 3 or P3	Means Incidents classified as Priority 3 (P3) meaning: • Failure of a Service that impacts a single Police User, for example: – a single Police User not able to login to xxxx, or – ??? • Failure or degradation of Service to multiple Police Users where an acceptable Workaround is in place.
Priority 4 or P4	Means incidents that are classified as Priority 4 (P4) meaning: • Non-urgent Incidents or Service Requests with minor impact (e.g. inconvenience) the resolution or fulfilment of which can be scheduled at a time agreed with User. • Incidents or Service Requests relating to test and development environments.

1.7 Attachments and References

The items detailed in these appendices are current at the time of signing this Agreement and are subject to on-going update through the Change Control Process or as specified in each appendix.

Appendix 1: xxx

Appendix 2: xxx

2. SCOPE OF SERVICES

2.1 Service Deliverables

The Service Provider will provide Support and Maintenance Services to ensure:

- Secure and reliable ICT Services and security of information in Police's ICT Operating Environment.
- The applicable Service Levels are met.
- Effective management and support of business as usual change in accordance with Police policy and standards to ensure that any such change has minimal impact on the Police ICT Operating Environment.
- Continuous Service improvement.
- Seamless integration with Police's Service Desk, Incident, Problem, Change, Release and Asset and Configuration Management processes.

2.2 Services

The following table outlines the Service Provider's tasks, functions and responsibilities in relation to the Support and Maintenance Services:

Item	Detailed Services Scope
1.	**Support Desk** The Service Provider will: a) Maintain a Support Desk which will accept, log, respond to and manage the Resolution of Incidents and Requests raised by Police. The Support Desk will be available to Police by telephone, email and via the Support Website. The Support Desk will be staffed by an adequate number of fully trained and adequately qualified Service Provider personnel. The contact details are as follows: Support Website: E-Mail: Telephone:
2.	**Incident Management** The Service Provider will: b) Ensure that incidents logged with the Police Service Desk are allocated an agreed priority based on the impact to Police, and assigned to the Service Provider's support group. c) Through the use of the Police Incident Management System, record all relevant incident information to assist with diagnosis, restoration and recovery, and provide updates to assigned Incidents in accordance with Support and Maintenance Procedures. d) Manage all assigned incidents and problems through to restoration, recovery and resolution to meet the agreed timeframes and the Service Levels, coordinating with Police Support Groups and Other Parties as required in accordance with the incident management procedures in the Procedures Manual. e) For any Incident where remediation responsibility is not immediately clear, perform Grey Area Diagnosis until such responsibility is clarified, then manage the handover of the incident resolution and recovery to the relevant Service Provider group, Police Support Group or Other Party, including providing all relevant information available to the Service Provider (e.g. diagnosis results). f) Consult with Police regarding any proposed remedial actions that may affect business activities and schedule activities to minimise business impact. To avoid doubt, the Service Provider must get Police's prior consent (not to be unreasonably withheld or delayed) to take any remedial action that may have a material affect on business activities. g) As required by Police, execute escalation procedures in accordance with the escalation procedures in the Procedures Manual. h) Manage the escalation of incidents and problems to manufacturers/vendors and, in

Item	Detailed Services Scope
	collaboration with the Service Provider's Service Desk, track technical assistance requests relating to challenges, incidents and problems with vendors. i) Manage the remediation (i.e. restoring the operation of the server, application or system to the standard required by Police) of incidents. j) Ensure the required updates and notifications are provided to the Service Provider's Service Desk for all Incidents to enable the Service Provider to meet its Service Levels and reporting requirements. k) As required, execute escalation procedures in accordance with the escalation procedures in the Procedures Manual. l) Contribute to Incident Reports for incidents as required by providing to the Police Problem Manager all relevant information known to the Service Provider as a result of the Support and Maintenance Services. m) If the Service Provider determines, in its reasonable judgment, that an Incident is caused by elements outside of the Service Provider's responsibility, the Service Provider will provide available diagnostic information (e.g. stack trace) and analysis (suspected cause and potential fix) to the relevant Police Support Group or Other Party.
3.	**Problem Management** The Service Provider will: a) Assist Police's Problem Manager by contributing to the problem management process by providing relevant information known to the Service Provider as a result of performing the Support and Mainteance Services. b) Use all reasonable endeavours to identify the root cause of problems and provide recommendations to Police's Problem Manager on how they can be resolved.
4.	**Production Change Management** The Service Provider will: a) Maintain accountability and coordinate with Police Support Groups and Other Parties to update all relevant Documentation in accordance with Police Production Change Management processes and the Support and Maintenance Procedures. b) All recurring maintenance activities will be recorded and treated as planned Change Requests. c) Plan outages (scheduled downtime) for maintenance and upgrades so as to minimise impact on Police's normal business operations. To avoid doubt, the Service Provider must get Police's prior consent (not to be unreasonably withheld or delayed) to undertake any maintenance and upgrades that may have an impact on Police's normal business operations. d) Review Change Requests, including: i. Risk Assessment – risks involved with implementing/not implementing the change (for example business and/or technical risks). ii. Implementation Plan – detailed step-by-step instructions on how to implement the change, and detailed list of all required media and files, including location. iii. Test Plan – detailed test scenarios, expected results, actual results and steps to test the production environment after the change is implemented. iv. Back Out Plan – detailed step-by-step instructions on how to restore the environment to its original configuration. Detailed list of all required media and files including location. and providing advice to Police in respect of those matters.
5.	**Production Change Implementation** The Service Provider will:

Item	Detailed Services Scope
	a) Perform planned, unplanned, scheduled and emergency system maintenance in accordance with the Support and Maintenance Procedures. b) Follow a pre-defined set of procedures associated with taking an approved software package and loading it into the Police ICT Operating Environment. c) Where the Service Provider owns the Change Request they will provide updates to the Documentation prior to the change being implemented. d) Configuration information will be obtained through the production change management process to keep inventory information current. The Service Provider will collect and maintain configuration and inventory information relating to the Support and Maintenace Services. e) During planned changes all events and effects related to the affected device(s) will be suppressed (e.g. turning off/disabling the alerts on the devices).
6.	**Maintenance and Repair** The Service Provider will: a) Coordinate the maintenance and repair of hardware by Other Parties as required by Police. b) Provide onsite hardware maintenance and repair for the hardware detailed in Appendix xx Maintenance and Repair of Hardware of this Schedule. c) Manage the escalation of problems to hardware manufacturers as required.
7.	**Infrastructure and Middleware Management** The Service Provider will: a) Develop and implement preventative maintenance policies to maintain client and server performance, reliability and availability and document the preventative maintenance policies in the Support and Maintenance Procedures. b) Proactively perform preventative maintenance tasks set out in the preventative maintenance policies on systems and middleware, both remotely and on site, taking into account the manufacturer's recommendations and best practices for the system and middleware. c) Implement all engineering changes and fixes designed to improve the safety and reliability of devices and software within appropriate timeframes to meet Service Levels. d) Verify that scheduled Service management tasks and processing are completed in the correct sequence, on time and remediate as necessary and in accordance with the Support and Maintenance Procedures. e) Manage and maintain infrastructure and middleware in compliance with Police's published policies and standards relevant to the Police ICT Operating Environment e.g. security and server hardening. f) Manage and maintain all Linux, Unix and Windows based operating systems and associated infrastructure in accordance with the Support and Maintenance Procedures. g) Provide infrastructure and middleware maintenance including installation, administering associated authentication systems, monitoring system operation, and maintaining effective message transport and directory synchronisation on all Operations Devices. h) Coordinate the maintenance and repair of Operations Devices by Other Parties as required by Police. i) Perform proactive system tuning to improve the performance, reliability and availability of the server environment and middleware. j) Run daily, weekly and monthly system and procedural checks in accordance with the Support and Maintenance Procedures. k) Proactively, and at Police's reasonable request, advise Police on the selection of devices and software, including identification of compatibility and maintenance

Item	Detailed Services Scope
	issues, and installation and environmental requirements related to ongoing use. l) Design and implement processes that are approved by Police to achieve standardisation of the server environment and middleware. m) Upgrade, change or increase the capacity for server system software and business applications e.g. CPU, disk, memory, where this does not require an outage, is a configuration change only, can be delivered remotely and no additional hardware is required.
8.	**Systems Monitoring and Event Management** The Service Provider will: a) Manage and monitor threshold alerts for monitored server, database and/or storage devices and software to ensure that the number of events or potential events (and their effects) are avoided or minimised. b) Manage and monitor critical system processes, rectify unexpected events and restart services, all according to Support and Mainteance Procedures. c) Assess the impact of system and application events and take appropriate action(s). d) Implement and maintain processes to allow automated and remote systems management of the server environment. e) Configure database monitoring to automatically generate and log incidents for problems. f) Maintain proactive monitoring and management to capture and identify incidents before they cause a business impact. g) Perform periodic checks on server systems and promptly advise Police of any increased workloads requiring additional system resource. h) Manage and monitor the xxx Environment including, but not limited to: i. Performance Monitoring – 24x365 monitoring of xxx and applications. ii. Predictive Monitoring – provision of event management reports, in accordance with the Support and Maintenance Procedures, which enable the Service Provider to identify patterns that may predict improperly tuned operating systems. iii. Performance and Availability Reporting – Provision of performance and availability reporting (those types to be determined by Police and notified to the Service Provider from time to time) based on performance data polled as part of event and performance monitoring, designated by the Service Provider, such as real time 24x365 reports, on-demand hourly, daily, weekly, and monthly historical reports and summary e-mail reports available daily, weekly or monthly. iv. Incident Management – Monitoring Events are promptly presented to an analyst for evaluation. Events which are confirmed by the Service Provider (acting reasonably) to be 'valid' constitute an Incident. i) Review and validate the monitoring configuration (i.e. the rules relating to thresholds for alerts) and determine if action needs to be taken on any Events. A collection of Events may represent a new Incident. If the Service Provider determines (acting reasonably) that a collection of Events does justify an Incident (i.e. tuning of a device is required), the Service Provider will generate an appropriately prioritised Incident.
9.	**Capacity and Performance Management and Planning** The Service Provider will: a) The Service Provider is responsible for effective capacity and performance management of Police's xxx Environment. b) The Service Provider is required to proactively monitor and plan for the capacity

Item	Detailed Services Scope
	and performance implications of both the Police xxx Environment to ensure that the Police xxx Environment and any change is not adversely affected as a result of capacity or performance issues. c) Contribute to the development and maintenance of a capacity and performance plan, including obtaining input from Police Support Groups and Other Parties where required, for the Police xxx Environment. d) Contribute to ensuring that software product licensing is monitored and provide advice to Police in order to optimise use of, and prevent any capacity issues relating to, software product licences. e) Pro-actively advise Police of any potential capacity and performance issues in respect of a change to the Police xxx Environment. f) Recommend appropriate solutions for resolution of any identified capacity and performance issues. g) Optimise the use of existing capacity. h) Attend regular capacity and performance management meetings with Police as reasonably requested.
10.	**Software Management** The Service Provider will: a) Evaluate supported software Patches, Minor Releases and de-support notices for software managed by the Service Provider regularly and make recommendations to Police in relation to the implementation of upgrades and new releases. b) Implement supported software Patches and Minor Releases in accordance with Support and Maintenance Procedures and Police Change Management procedures. Software Patches will be implemented using remote management tools, to the extent possible. c) Proactively, and on reasonable demand, advise Police and relevant Other Parties about software compatibility issues related to ongoing use. d) Maintain the security, availability and performance of infrastructure and middleware applications supported e.g. Websphere, MQ Series
11.	**Database Management** The Service Provider will: a) Proactively manage and monitor the availability, security and integrity of Police's xxx databases such that preventative actions can be taken to avoid outages or deteriorations in availability, security or integrity. b) Field ad hoc database administration queries from Police and Other Parties, in liaison with vendors and Other Parties as required by Police. c) Monitor database product licensing and provide advice in order to optimise the use of, and prevent any capacity issues relating to, database product licenses. d) Execute database creation, configuration, and schema changes. e) Manage and monitor the performance and capacity of Police's xxx databases such that preventative actions by the Service Provider can be taken to avoid outages or deteriorations in performance or capacity. f) Execute existing automated test data refresh processes as required in the Support and Maintenance Procedures.
12.	**Information Security Management** The Service Provider will: a) Provide and maintain information security standards, and processes. b) Ensure compliance with baseline security standards and processes. c) Perform 3 monthly security audits to ensure that the Service Provider and the Police xxx Environment comply with the Information Security Policy & Standards,

Item	Detailed Services Scope
	for example, DBA access reviews, redundant user reviews. d) Undertake the oversight of vulnerability mitigation and reporting as advised by Police Security staff. e) Ensure that security vulnerability patching complies with Police's Information Security policy and associated standards, and is performed promptly and accurately. f) Provide support for Police internal and external security audits g) Provide assistance to Police Service provider 3rd parties in relation to the performance of regular security audits and ethical hacks across the Police xxx Environment. h) Promptly install security patch files to operating systems, databases etc. as they are made available by the manufacturer. i) Provide a vulnerability alerting service for the Police software inventory and enter details in the ICT Security Risk Register. The vulnerability remains in the register until all patching to remediate the risk is completed. j) Upon detection or notification of a security incident or new potential risk, work with Police to: i. Notify affected parties. ii. Assess the scope of any loss of or damage to systems; or the compromise, or potential compromise, of data. iii. Contain the threat, or potential threat. iv. Take steps to salvage/restore as much of impacted server, data and software as possible within the limitations of the software/devices available. v. Take all other remedial action and mitigation steps as necessary or appropriate. vi. Provide appropriate incident reporting to Police ICT Security staff. k) Provide routine and ad-hoc reporting to Police on security matters. l) Oversee computer media sanitisation/destruction as part of a storage, handling and disposal process.
13.	**Storage, Data Protection and Recovery** The Service Provider will: a) Manage and monitor the file systems, allocation and components of direct attached storage (DAS) devices, Network-Attached Storage (NAS) arrays and Storage Area Networks (SAN), including associated service processors and disk controllers. In addition, manage the SAN controlling application, which controls advanced storage features e.g. snapshots and mirror copies; and will monitor the SAN fabric that connect hosts to storage. b) Configure storage management to optimise performance, availability, scalability and redundancy where possible within the architecture applied. c) Contribute any current or potential storage capacity issues with recommendations on how they can be resolved. d) Regularly initiate and complete required processing management functions to ensure physical integrity of data. e) Manage and monitor (success, failure, issues) on all replication, synchronisation and backup jobs; equipment and resources, and initiate appropriate action(s) if scheduled backups have failed. f) Define and comply with backup schedules, datasets, retention periods, levels (i.e. full, incremental, or differential) in accordance with Police backup and recovery policies and standards. g) Perform operational data restoration as required by Police, and schedule data

Item	Detailed Services Scope
	restoration so as to minimise impact on normal operations and Police's day-to-day business. To avoid doubt, the Service Provider must get Police's prior consent (not to be unreasonably withheld or delayed) to perform operational data restoration that may have a material affect on Police's day to day business. Further, where Police has requested a delay to the restoration of data, that delay should not count towards the Service Provider's achievement of the Service Levels. h) Provide advice to the Police Capacity Manager of any current or potential backup capacity issues (including media requirements) with recommendations on how they can be resolved. i) Manage and monitor data replication between systems in the Police Operating Environment. j) In accordance with the problem management procedures set out in the Support and Maintenance Procedures, identify the root cause of recurring backup failures and provide recommendations to Police on how they can be resolved. k) Perform periodic test restores for each backup device in accordance with Support and Maintenance Procedures. Such tests will be scheduled so that a backup from each device is tested at least once annually, and after any significant system changes. l) Manage tape operations and administration for all supported devices at Police Hosting Data Centres and other locations including preparation of tapes for shipment to agreed schedules in collaboration with Other Parties. m) Ensure data integrity, and confidentiality, is maintained and available as architected in the Support and Maintenance Procedures.
14.	**Service Quality and Reporting** The Service Provider will: a) Comply with Police's published policies, standards and procedures in the delivery of all Operations Services e.g. Police Information Security policy, standards and procedures. b) Ensure the Service Levels are implemented, kept current and being met. c) Actively foster collaboration principles when interacting with Police Support Groups and Other Parties. d) Proactively identify and scope improvements to the Support and Maintenance Services including: i. Improvements to service quality aligned with Police's stated ICT business objectives. ii. Improvement of efficiency and elimination of waste through the streamlining of operational processes and procedures. e) Maintain accountability and coordinate with Other Parties to ensure delivery of the Services to the agreed Service Levels and in accordance with Police policies and standards and the Support and Maintenance Procedures. f) Provide input to and contribute source data to the Support and Maintenance reporting as reasonably required to ensure that the Service Provider's reporting requirements are met. g) Provide report statistics for monthly reporting sufficient to meet the reporting requirements. h) Provide Police and Other Parties with access to configuration data including performance and availability information. i) Provide daily, weekly and monthly backup reporting. e.g. backup success and failure, growth in backup times, growth in backup volumes in accordance with the Support and Maintenance Procedures. j) Provide event management reports, updated every hour and containing the most

Item	Detailed Services Scope
	recent thirty days of data collected, organised by device, date and event type.

2.3 **In-scope Additional Services**

The following Services are within scope of the Support and Maintenance Services but they may incur additional charges (as set out in clause 10.1(b) of this Schedule):

Item	Additional Services Scope	Charge
1.	Repair of out of warranty hardware where approved by Police.	Time and Materials
2.		
3.		
4.		

2.4 **Out of Scope Services**

The following Services are out of scope of the Support and Maintenance Services:

Item	Out of Scope Services	Responsibility
1.	Change projects (for example development or significant change projects) are outside the scope of Support and Maintenance Services except where, by prior agreement of Police, the change can be implemented and completed within capability and workload of the Service Provider's Key Roles without impacting any other Police Services. Change projects will normally be resourced and funded separately at the sole discretion of Police.	To be determined by Police
2.		
3.		

2.5 **Service Notes**

a) The interfaces, roles and responsibilities of the Service Provider, Police Support Groups and Other Parties in relation to their respective services and the Support and Maintenance Services do not in any way restrict the obligation on the Service Provider to perform the Support and Maintenance Services.

3. POLICE ROLES AND RESPONSIBILITIES

With respect to the Services described in this Schedule, Police will:

a) Allow and enable the Service Provider to supply Services remotely (i.e. off-site from Police's premises), with connectivity to the Police network provided by VPN, remote access or fixed line, provided that the Service Provider:

i. is responsible for providing all Service Provider located devices and other equipment necessary to enable the supply of remote Services; and

ii. where appropriate, supplies the Services onsite.

b) Manage and maintain the Police change management process (CR).

c) Where required, maintain current manufacturer warranty, maintenance and service contracts.

d) Acting reasonably, permit the Service Provider to install management and monitoring software and infrastructure e.g. monitoring tool agents, Control Tower appliances, in accordance with relevant Police policies, standards and procedures.

e) Provide final approval of the technology direction, architecture and design.

f) In a timely manner, inform and consult with the Service Provider on changes in business objectives that could impact the Service Provider's Services.

g) Maintain physical access procedures and ensure the Service Provider has access to Police sites and Hosting Data Centres as appropriate.

h) Where practicable, ensure contractual arrangements are aligned which encourage collaboration between the Service Provider and Other Parties so that the Service Provider is not unreasonably withheld from complying with the relevant service and associated Service Levels. To avoid doubt, this clause does not require Police to amend and contract in force at the date of this Agreement.

4. SERVICE PROVIDER ROLES AND RESPONSIBILITIES

With respect to the Services described in this Schedule, the Service Provider will:

a) Provide the Support and Maintenance Services to Police in accordance with this Schedule, including the Service Levels and Support and Maintenance Procedures.

b) Collaborate with Police Support Groups and Other Parties to facilitate achievement of the Police Support Groups and Other Parties service levels.

c) Adhere to published Police policies, standards and processes applicable to the support of the Support and Maintenance Services.

5. SERVICE LEVELS AND MEASURES

5.1 Hours of Support

a) Unless specified in another Schedule and with the exception of scheduled outages, the Operations Services will be available as follows:

Support Service	Weekdays	Weekend and National Public Holidays
Support Desk	24 hours per day	n/a

5.2 Service Level Measures

a) The following Service Levels will apply to the Support and Maintenance Services:

Include the Service levels appropriate to the services

Availability	
Description	The number of hours that the xxxx are available for use during each reporting period.
Purpose	To ensure the xxxx are available for use by Police as required.
Service Level	99.9% availability for the xxxx 24 x 7.

Measurement Point	Measured from the time Police logs an Incident with the Service Provider until the Incident is Restored to Service or Resolved.
Calculation	The total time in hours during which the xxx are unavailable for use during each reporting period divided by the total possible hours of availability of the xxxx during that reporting period, and expressed as a percentage. The calculation excludes scheduled preventive maintenance requirements.
Calculation Frequency	Monthly

Incident Response	
Description	Response time to Priority One or Priority Two Incidents logged by Police are met within: **Incident Priority** / **Response Timeframe** Priority One: Within 15 minutes Priority Two: Within 30 minutes Priority Three: n/a Priority Four: n/a
Purpose	To ensure the timely Response to Major Incidents.
Service Level	100% of Priority One and Priority Two Incidents are Responded to within the timeframes specified in the Incident Response Description.
Measurement Point	Measured from the time Police logs a Priority One or Priority Two Incident with the Service Provider and the time the Service Provider provides the Incident Response.
Calculation	The number of Priority One or Priority Two Incidents logged by Police to the Service Provider in the reporting period that are Responded to within the timeframes specified in the Incident Response Description, divided by the total number of Priority One or Priority Two Incidents logged by Police to the Service Provider in the reporting period, and expressed as a percentage.
Calculation Frequency	Monthly

Incident Updates	
Description	The Service Provider's provision of Incident updates are met within: **Incident Priority** / **Update Timeframe** Priority One: At 30 minute intervals following the Incident Response Priority Two: At 60 minute intervals following the Incident Response Priority Three: As agreed with the User Priority Four: As agreed with the User
Purpose	To ensure timely Communication of Updates for the duration of the Incident.
Service Level	100% of Priority One Incident Updates are provided within the timeframes specified in the Incident Update Description; 100% of Priority Two Incident Updates are provided within the timeframes specified in the Incident Update Description; 90% of Priority Three Incident Updates are provided within the timeframes specified in the Incident Update Description; and

Incident Updates	
	90% of Priority Four Incident Updates are provided within the timeframes specified in the Incident Update Description.
Measurement Point	Measured for Priority One and Two Incidents from the provision of the Incident Response to the time the Service Provider provides the Incident Updates. Measured for Priority Three and Four Incidents from the acknowledgement of the receipt of the Incident by the Service Provider to the time the Service Provider provides the Incident Updates.
Calculation	The number of Incident Updates in the reporting period that are provided within the timeframes specified in the Incident Update Description, divided by the total number of Incident Updates in the reporting period, and expressed as a percentage.
Calculation Frequency	Monthly

Incident Restoration of Service	
Description	The total time taken by the Service Provider to implement a Workaround and Restore Service is met within:

Incident Priority	Restoration of Service Timeframe	Restoration of Service Timeframe On Call
Priority One	2 Business Hours	4 hours
Priority Two	4 Business Hours	6 hours
Priority Three	1 Business Day	n/a
Priority Four	n/a	n/a

Purpose	To ensure the timely implementation of Workarounds to Restore Services.
Service Level	95% of Priority One Incident Restoration of Service within the timeframe specified in the Incident Restoration of Service Description; 95% of Priority Two Incident Restoration of Service within the timeframe specified in the Incident Restoration of Service Description; and 95% of Priority Three Incident Restoration of Service within the timeframe specified in the Incident Restoration of Service Description.
Measurement Point	Measured from the time Police logs an Incident with the Service Provider until the Incident Restoration of Service is complete.
Calculation	The number of Incidents logged by Police to the Service Provider during the reporting period which are Restored to Service within the timeframes specified in the Incident Restoration of Service Description divided by the total number Incidents logged by Police to the Service Provider during the reporting period, and expressed as a percentage.
Calculation Frequency	Monthly

Incident Resolution	
Description	The total time taken by the Service Provider to Resolve an Incident is met within:

Incident Priority	Resolution Timeframe
Priority One	30 Business Days
Priority Two	30 Business Days
Priority Three	30 Business Days
Priority Four	n/a

Incident Resolution	
Purpose	To ensure the timely Resolution of Incidents.
Service Level	99% of Priority One Incidents Resolved within the timeframe specified in the Incident Resolution Description; 95% of Priority Two Incidents Resolved within the timeframe specified in the Incident Resolution Description; 95% of Priority Three Incidents Resolved within the timeframe specified in the Incident Resolution Description; and 90% of Priority Four Incidents Resolved within the timeframe specified in the Incident Resolution Description.
Measurement Point	Measured from the time Police logs an Incident with the Service Provider until the Incident is Resolved.
Calculation	The number of Incidents logged by Police to the Service Provider during the reporting period which are Resolved within the timeframes specified in the Incident Resolution Description divided by the total number Incidents logged by Police to the Service Provider during the reporting period, and expressed as a percentage.
Calculation Frequency	Monthly

5.3 **Service Level Rebates**

a) In addition to any other rights or remedies Police may have under this Agreement or at law, the Service Provider agrees to pay the following rebates in relation to its failure to meet or exceed the Key Service Levels.

b) Service Level Rebates apply in relation to Service Level Defaults for Key Service Levels, as detailed in the table below. Up to two levels of Service Level Credit may apply to each Critical Service Level, linked to the severity of the Service Level Default.

c) A Service Level Default does not apply where an action or inaction by third party or Police personnel materially contributed to the default.

d) If one event triggers two or more Service Level Defaults then only the Service Level Default with the highest Service Level Credit will apply.

e) The Service Level Rebate is specified in terms of a percentage of the monthly Support and Maintenance Services Charges.

f) The Key Service Levels are as detailed in the following table:

Key Service Level	Service Level Default	Service Level Rebate
Availability	Between 95% and 99.9% Less than 95%	1% 2%
Incident Restoration of Service	Less than 95% of P1 and P2 Incidents are Restored to Service within the agreed timeframes	1%

6. SERVICE DISENGAGEMENT

6.1 Should Police terminate this Schedule, the disengagement requirements are specified in clause 17 of the Master Agreement.

7. DOCUMENTATION

The Service Provider will:

7.1 Develop, manage and maintain Documentation for the Support and Maintenance Services including:

a) Support and Maintenance Procedures

b) Relevant knowledge base entries.

c) Relevant known errors.

d) Technical and hardware Documentation, including infrastructure diagrams and processes.

e) Documentation relating to Operations interfaces, roles and responsibilities with Police Support Groups and Other Parties

7.2 Annually audit the Documentation for completeness and accuracy and update that Documentation where it is incomplete or inaccurate.

7.3 Provide Police and Other Parties with access to current and archived copies of Documentation and records relating to Operations Services as required by Police.

7.4 Provide Documentation in the format reasonably required by Police.

7.5 Save and archive agreed Documentation and records in a retrievable, readable format. All arrangements related to archiving of Documentation and records are to be approved by Police, including the format, medium, timeframe and process for archiving.

8. KEY ROLES

8.1 The following Key Roles will form the Service Provider's core team to ensure the provision of the Support and Maintenance Services:

Role	FTE	Type
	1	Dedicated
	1	Dedicated
Total	**2**	

8.2 Sufficient Service Provider personnel will be assigned as required to deliver the Support and Maintenance Services to Police in accordance with this Agreement. These personnel will be appropriately knowledgeable, skilled and trained in dealing with Police Incidents and Service Requests and the Police ICT environment and trained to be familiar with Police.

9. TRAINING

9.1 The Service Provider will provide training of all relevant Service Provider personnel, as required, to implement and maintain the Services within the scope of this Schedule to the required Service Levels.

9.2 The Service Provider will ensure all staff maintain current skills to provide the Support and Maintenance Services and attend certified training courses associated with any major product releases/upgrades to operating systems, server and storage infrastructure products.

9.3 The Service Provider will ensure that it maintains relevant vendor certifications e.g. HP qualifications to support the Police ICT Operating Environment in accordance with this Agreement.

10. SUPPORT AND MAINTENANCE SERVICES PRICE

10.1 Charges

a) The following pricing model applies to all of the Support and Maintenance Services except the In-scope Additional Services:

Insert pricing table

b) The In-scope Additional Services specified in clause 2.3 as Time and Materials will be charged separately as detailed in the Service Provider Service Rates.

10.2 **Pricing Notes**

a) All hardware is procured with the appropriate manufacturers onsite parts and labour warranty program.

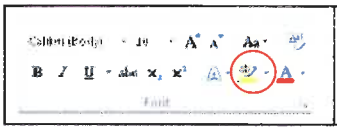
APPENDIX 1: XXX

The information in this appendix is current at the time of Commencement and will be updated on a regular basis and stored in a secure location on Police's network for the storage of shared Documentation.

RFP Response Form

Instructions for Respondents

- Please use this Response Form in responding to our RFP. It is important that you do not change the structure (section headings and sequence). Changing this structure will make it harder for the evaluators to find relevant information quickly.
- Before starting to complete this form please make sure that you have read the Request for Proposals (RFP) in full and understand our Requirements (RFP Section 2), our Evaluation Approach (RFP Section 3) and the RFP Process, Terms and Conditions (shortened to RFP-Terms described in Section 6). If anything is unclear or you have any questions please get in touch with our Point of Contact (RFP Section 1 paragraph 1.3) before the Deadline for Questions (RFP Section 1, paragraph 1.2).
- We have included supplier tip boxes to help you understand what is required. The areas highlighted in yellow indicate where you are to write your response.
- Remember to delete the supplier tip boxes and remove the highlight from your answers before sending us your response – they are for your use only!

	To remove highlight from text: select the text you want to remove the highlight from. In the 'Home' tab in the 'Font' group select the arrow at the right of the 'Text highlight colour' and select 'no colour'.

- For more general information on how to respond to tenders refer to the suppliers' resource centre at: www.procurement.govt.nz/for suppliers.

Check list for Respondents

Task	✓
1. Complete all sections of the Response Form.	
2. Delete all 'supplier tip' boxes from the Response Form. 3. Remove all yellow highlight from the Response Form.	
4. Make sure that you have complied with the following instructions: • 'two envelope system': provide all financial information relating to price, expenses and costs in a separate sealed envelope/soft copy folder. • the font used is Calibri font size 11.	
5. Arrange for the declaration to be signed.	
6. Prepare your Proposal for delivery by arranging the printing of one signed hard copy original AND creating a final soft copy file copied to a USB storage device. 7. Where both hard and soft copies have been requested double check that the hard copies and soft copy are identical.	
8. Arrange for the Proposal to be delivered before the Deadline for Proposals.	

[insert your organisation name and logo or branding]

Response Form

In response to Request for Proposals

by: New Zealand Police

for: ABIS 2

ref: RFP TN/18/03 – ABIS 2

Date of this Proposal: [insert date of this document]

Supplier tips

Words and phrases that have a special meaning are shown by the use of capitals e.g. Respondent, which means '*a person, organisation, business or other entity that submits a Proposal in response to the RFP. The term Respondent includes its officers, employees, contractors, consultants, agents and representatives. The term Respondent differs from a supplier, which is any other business in the market place that does not submit a Proposal*'. Definitions are at the end RFP Section 6.

1. About the Respondent

Supplier tips

- The section gives the Buyer basic information about your organisation and identifies your Point of Contact for the duration of the RFP process.
- If an item is not applicable e.g. you do not have a registered office complete the box by stating 'not applicable'.
- If you are submitting a joint or consortium Proposal complete an 'Our profile' table for each Respondent. Cut and paste the table as appropriate. Provide only one Point of Contact for your joint/consortium Proposal.

Our profile

Choose one of these statements to complete, and delete the others

This is a Proposal by [insert the name of your organisation] (the Respondent) alone to supply the Requirements.

OR This is a [joint/consortium] Proposal, by [insert the name of your organisation] and [insert the name of the other organisation/s] (together the Respondents) to supply the Requirements.

Item	Detail
Trading name:	[insert the name that you do business under]
Full legal name (if different):	[if applicable]
Physical address:	[if more than one office – put the address of your head office]
Postal address:	[e.g. P.O Box address]
Registered office:	[if you have a registered office insert the address here]
Business website:	[url address]
Type of entity (legal status):	[sole trader / partnership / limited liability company / other please specify]
Registration number:	[if your organisation has a registration number insert it here e.g. NZBN, company registration number]
Country of residence:	[insert country where you (if you are a sole trader) or your organisation is resident for tax purposes]
GST registration number:	[NZ GST number / if overseas please state]

Our Point of Contact

Item	Detail
Contact person:	[name of the person responsible for communicating with the Buyer]
Position:	[job title or position]
Phone number:	[landline]
Mobile number:	[mobile]

Email address:	[work email]

Other information

Item	Detail
Will any subcontractors be involved?	[YES / NO] If yes, specify for each subcontractor: Who?: Value involved?: Extent of tasks involved?: (Attach information if not enough room here)
What warranties will apply?	[warranties]
Are you ISO 9000 series certified?	[YES / NO] If yes, what series?: If no, other system used?:
When were you last independently audited?	[date] [by]
Is any licence / permit or other authorisation required?	[YES / NO] If yes, specify:

2. Response to the Requirements

Supplier tips

- In this section you are asked to provide your response to our Requirements (RFP Section 2) by demonstrating your organisation's ability to meet our criteria (RFP Section 3: Our Evaluation Approach). Carefully read RFP Sections 2 and 3 before completing this part.
- If there is anything that you do not understand ask our Point of Contact to clarify.
- If any information you provide is commercially sensitive to your business you must let the Buyer know. Please mark the information 'commercially sensitive' or 'Confidential Information'. It is not acceptable to render this whole document confidential unless this is truly the case. The Buyer has a duty to protect Confidential Information, subject to the exceptions in the RFP-Terms (Section 6).
- If some of an answer is in another document e.g. a marketing brochure, copy and paste the relevant extract into this Proposal. Do not submit the whole brochure. Please do not include any advertising brochures or similar material in your Proposal.
- You may include information not specifically requested by us in your Proposal. But only if it adds value and is relevant to the Requirements.

Pre-conditions

Supplier tips

- You must be able to answer 'yes' to each of these pre-conditions. Make sure you are able to verify that this is the case, if asked.
- 'Yes' means that you can currently meet the pre-condition. It does not mean that you are planning to, or intend to at some time in the future.
- If you cannot answer 'yes' to all, your Proposal will not meet the basic Requirements and will be declined.

#	Pre-condition	Meets
1.	There are no specific preconditions relating to this RFP however Respondents should note that there are multiple Mandatory Requirements for the solution detailed in the Detailed Requirements Document. Respondents should familiarize themselves with the Mandatory aspects of the solution prior to responding to this RFP and ensure the proposed solution meets those Mandatory requirements.	[Yes/No]

Questions relating to the evaluation criteria

Supplier tips

- Here you are asked to answer questions relating to the evaluation criteria. Your Proposal will be scored against your answers to these criteria. Aim to give answers that are relevant, concise and comprehensive.
- Consider the % weighting for each criterion. The higher the weighting the more important it is. Take the weightings into account in deciding how much detail to include.
- If you have made any assumption about the Requirements or delivery, clearly state the assumption.
- There may be several questions that relate to one criterion. If these questions are not individually weighted assume that they are of equal importance.

Please used the attached **Requirements Response Form** to respond to the questions relating to the evaluation criteria.

3. Price

Supplier tips

- In the RFP Section 4 we have outlined the pricing information that we are seeking. This should inform you how to present your proposed price. Where we have provided a template you must use this for your pricing information.
- In preparing your pricing information you must consider all risks, contingencies and other circumstances relating to the delivery of our Requirements and include adequate provision for them. You must also document any assumptions that you have made in costing the full delivery of the Requirements.
- If asked for a 'whole-of-life' cost this is the total cost to the Buyer over the whole of the life of the Contract. See Guide to Total Cost of Ownership and TCO calculator (listed under 'T').
- If we have asked for a two envelope response you must put all financial and pricing information in a separate sealed envelope or separate soft copy document.

Price as a weighted criterion

1. Value for money (based on whole-of-life cost)	Weighting 30%
e.g. Provide the total price and a breakdown of the total costs over whole-of-life of the Contract.	100%
e.g. Detail any other cost and benefits.	

Pricing schedule

Please submit your financial information and pricing using the pricing template provided (Excel spreadsheet).

Assumptions

Please state any assumptions you have made in relation to the cost and pricing information.

[Insert Pricing assumptions]

4. Proposed Contract

Supplier tips

- In the RFP Section 5 we have detailed the terms and conditions of our Proposed Contract. We need to know whether or not you are prepared to do business based on the Proposed Contract.
- If you have any points that you wish to make about the Proposed Contract this is where you tell us. Note below any suggestions or changes you wish to propose.
- It is important that, if asked, you are able to explain why your changes are important to you.
- In deciding which Respondent/s to shortlist the Buyer will take into account each Respondent's willingness to meet the Proposed Contract terms and conditions.

Choose one and delete the other:

Having read and understood the Proposed Contract, in the RFP Section 5, I confirm that these terms and conditions are acceptable. If successful, I agree to sign a Contract based on the Proposed Contract, or such amended terms and conditions of Contract as are agreed with the Buyer following negotiations. OR

Having read and understood the Proposed Contract, in the RFP Section 5, I have the following suggestions to make. If successful, I agree to sign a Contract based on the Proposed Contract subject to negotiating the following clauses:

Clause	Concern	Proposed solution
[insert number]	[briefly describe your concern about this clause]	[describe your suggested alternative wording for the clause or your solution]
[insert number]	[briefly describe your concern about this clause]	[describe your suggested alternative wording for the clause or your solution]

5. Referees

Supplier tips

- Here you are asked to provide the names and contact details of your referees. These must be work related referees i.e. not a friend or family member.
- The best referees are those for whom you have recently delivered similar goods or services.
- Before including their details check with them to make sure that they consent to acting as referee on behalf of your organisation.

Please supply the details of two referees for your organisation. Include a brief description of the goods or services that your organisation provided and when.

Please note: in providing these referees you authorise us to collect any information about your organisation, except commercially sensitive pricing information, from the referees, and use such information in the evaluation of your Proposal. You also agree that all information provided by the referee to us will be confidential to us.

First referee	
Name of referee:	[insert name of the referee]
Name of organisation:	[insert name of their organisation]
Goods/services provided:	[brief description of the goods/services you provided to this referee]
Date of provision:	[insert the date when you provided the goods/services]
Address:	[insert street address]
Telephone:	[insert mobile or landline]
Email:	[insert email address]

Second referee	
Name of referee:	[insert name of the referee]
Name of organisation:	[insert name of their organisation]
Goods/services provided:	[brief description of the goods/services you provided to this referee]
Date of provision:	[insert the date when you provided the goods/services]
Address:	[insert street address]
Telephone:	[insert mobile or landline]
Email:	[insert email address]

Please contact me before you approach a referee for a reference	Yes/Not required

6. Our declaration

Supplier tips

- Here you are asked to answer questions and make a formal declaration.
- Remember to select 'agree' or 'disagree' at the end of each row. If you don't you will be deemed to have agreed.
- Remember to get the declaration signed by someone who is authorised to sign and able to verify each of the elements of the declaration e.g. chief executive or a senior manager.
- If you are submitting a joint or consortium Proposal each Respondent (supplier involved in the joint or consortium Proposal) must complete a separate declaration.

Respondent's declaration		
Topic	**Declaration**	**Respondent's declaration**
RFP Process, Terms and Conditions:	I/we have read and fully understand this RFP, including the RFP Process, Terms and Conditions (shortened to RFP-Terms detailed in Section 6, as amended by Section 1, paragraph 1.6. if applicable). I/we confirm that the Respondent/s agree to be bound by them.	**[agree / disagree]**
Collection of further information:	The Respondent/s authorises the Buyer to: a. collect any information about the Respondent, except commercially sensitive pricing information, from any relevant third party, including a referee, or previous or existing client b. use such information in the evaluation of this Proposal. The Respondent/s agrees that all such information will be confidential to the Buyer.	**[agree / disagree]**
Requirements:	I/we have read and fully understand the nature and extent of the Buyer's Requirements as described in Section 2. I/we confirm that the Respondent/s has the necessary capacity and capability to fully meet or exceed the Requirements and will be available to deliver throughout the relevant Contract period.	**[agree / disagree]**
Ethics:	In submitting this Proposal the Respondent/s warrants that it: a. has not entered into any improper, illegal, collusive or anti-competitive arrangements with any Competitor b. has not directly or indirectly approached any representative of the Buyer (other than the Point	**[agree / disagree]**

	of Contact) to lobby or solicit information in relation to the RFP c. has not attempted to influence, or provide any form of personal inducement, reward or benefit to any representative of the Buyer.	
Offer Validity Period:	I/we confirm that this Proposal, including the price, remains open for acceptance for the Offer Validity Period stated in Section 1, paragraph 1.6.	**[agree / disagree]**
Conflict of Interest declaration:	The Respondent warrants that it has no actual, potential or perceived Conflict of Interest in submitting this Proposal, or entering into a Contract to deliver the Requirements. Where a Conflict of Interest arises during the RFP process the Respondent/s will report it immediately to the Buyer's Point of Contact.	**[agree / disagree]**

Details of conflict of interest: [if you think you may have a conflict of interest briefly describe the conflict and how you propose to manage it or write 'not applicable'].

DECLARATION

I/we declare that in submitting the Proposal and this declaration:

a. **the information provided is true, accurate and complete and not misleading in any material respect**
b. **the Proposal does not contain intellectual property that will breach a third party's rights**
c. **I/we have secured all appropriate authorisations to submit this Proposal, to make the statements and to provide the information in the Proposal and I/we am/are not aware of any impediments to enter into a Contract to deliver the Requirements.**

I/we understand that the falsification of information, supplying misleading information or the suppression of material information in this declaration and the Proposal may result in the Proposal being eliminated from further participation in the RFP process and may be grounds for termination of any Contract awarded as a result of the RFP.

By signing this declaration the signatory below represents, warrants and agrees that he/she has been authorised by the Respondent/s to make this declaration on its/their behalf.

Signature: _____

Full name: _____

Title / position: _____

Name of organisation: _____

Date: _____

Requirements Response Form

1 Solution Overview

1.1 The Respondent shall provide an overview of the solution being proposed, that describes:

ID	DETAIL
1.1.1	Overall system architecture. The inclusion of any diagrams would be beneficial.
[insert your answer here]	
1.1.2	Major functional and technical components, features and integration points.
[insert your answer here]	
1.1.3	Interfacing capabilities and protocols.
[insert your answer here]	
1.1.4	Security control mechanisms.
[insert your answer here]	
1.1.5	Scalability of the solution.
[insert your answer here]	
1.1.6	Communication middle-ware required/supported, including wired and wireless local area and wide area networking protocols required or supported.
[insert your answer here]	
1.1.7	Preferred enterprise management tools (if any) and the roles such tools might play in the solution.
[insert your answer here]	
1.1.8	Additional hardware and software required to support the system.
[insert your answer here]	
1.1.9	Disaster Recovery.
[insert your answer here]	
1.1.10	Non production environments including any constants or limitations or restrictions that apply to them.
[insert your answer here]	

2 Solution Development

ID	DETAIL

2.1	The Respondent shall describe their problem management, release management, and change management processes for the device and software.
[insert your answer here]	
2.2	The Respondent shall provide a change history of past releases over the last three years for the device and software with dates and descriptions of major functional and technical enhancements.
[insert your answer here]	
2.3	The Respondent shall provide an outline of the planned development and release schedule for the device and software up to and including the next 24 months, and what functional and technical enhancements are expected within those releases.
[insert your answer here]	
2.4	The Respondent shall describe their organisation's approach to supporting past versions of the software solution, and in assisting customers to migrate to new releases.
[insert your answer here]	

3 Flexibility

ID	DETAIL
3.1	The Respondent shall describe how flexible the solution is to customise specific integration and export and import features/functions for NZ Police such that the solution can be upgraded easily, and with minimal impact and cost, to incorporate those Police specific features.
[insert your answer here]	
3.2	The Respondent shall describe how any features requested by NZ Police for their solution are made and released.
[insert your answer here]	
3.3	The Respondent shall describe any new function (including upgrades or new versions of their current device) which they are in the process of developing or have recently developed, if not yet available.
[insert your answer here]	

4 Deployment and support

4.1 The Respondent shall provide an overview that describes:

ID	DETAIL
4.1.1	Proactive monitoring and support of the solution.
[insert your answer here]	
4.1.2	Approach to initial deployment of the solution

[insert your answer here]	
4.1.3	Approach to managing future releases within the production and non-production environments.
[insert your answer here]	
4.1.4	Outline the future roadmap for product delivery and development
[insert your answer here]	

5 FUNCTIONAL REQUIREMENTS

5.1 Image Integrity - User Activity Log

ID	DETAIL
IU1	It is mandatory that the system(s) will provide a user activity log. This may include but is not limited to the following: • Date/time and user who imported, updated, enhanced an image; and entered or updated its associated metadata. • Date/time and user who destroyed an Image. • Date/time and user who added or removed an image from a watch list. • Date/time and user who created an electronic line-up or photobook • Date/time and user who used an image in a line-up, photobook or exported the image. • Date/time the user created, used in viewing an electronic photobook The user activity log is visible to authorised users within the application.
[insert your answer here]	
IU2	It is mandatory that a user may view the artefact related to the object/image that they are viewing.
[insert your answer here]	

5.2 Image Integrity – Image Alteration

ID	DETAIL
IA1	The original image(s) stored by the image management system cannot be altered and storage meets the recommendations below. It is mandatory that the images must be safeguarded against alteration of the original images. Outline how your solution provides this safeguard. References: http://www.anzpaa.org.au/ArticleDocuments/282/2013%20Australia%20and%20New%20Zealand%20Guidelines%20for%20Digital%20Imaging%20Processes.pdf.aspx http://www.anzpaa.org.au/about/general-publications/guidelines-for-digital-imaging-processes.
[insert your answer here]	
IA2	It is mandatory that a working copy of the original image will be the image used for enhancement purposes, and that a link between the working copy and original image will be held and evident.
[insert your answer here]	

5.3 Image Management

ID	DETAIL
IM1	It is mandatory that the system(s) has/have the capacity to use unique keys for accessing of or by other systems retaining these as metadata against an image(s).
[insert your answer here]	
IM2	It is mandatory that images held meet ANSI/NIST minimum standard. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-290e2.pdf https://fiswg.org/FISWG_CaptureAndEquipmentAssessmentForFRSystems_v1.0_2011_05_05.pdf
[insert your answer here]	
IM3	It is mandatory that an authorised user has/have the ability to multiple select / discard images (facial, SMT and clothing) prior to permanent storage in system. Eg re scan an original image that did not initially scan correctly.
[insert your answer here]	
IM4	It is mandatory that an authorised user has the ability to correct the metadata associated to an image.
[insert your answer here]	
IM5	It is mandatory that the system will retain the original image without compression, ensuring the storage of the best quality image.
[insert your answer here]	
IM6	It is mandatory that the system(s) has/have the ability to lock stored images, both the original and each subsequent working copy to prevent alteration.
[insert your answer here]	
IM7	It is mandatory that an authorised user has the ability to export stored images to external media.
[insert your answer here]	
IM8	It is mandatory that the system(s) has/have the ability to store the following as separate images: (i) Facial -frontal (ii) Facial - Profile (iii) Full Body (iv) SMT - Scars, Marks, Tattoos
[insert your answer here]	
IM9	It is desirable that the system(s) has/have the ability to store the following as separate images: (i) Clothing logo

[insert your answer here]	
IM10	It is mandatory that all images must have a unique reference number.
[insert your answer here]	
IM11	It is mandatory that authorised user may destroy an image or set of images, including the original. If the image has been used as a filler in the line-up the line-up is flagged to prevent being re-used. NOTE: S.34 Policing Act governs destruction of originals and associated working copy images (except for images used in a line-up) captured under section 32 and 33 of the Policing Act. Child Protection (Child Sex Offender Government Agency Registration) Act 2016 governs the destruction of originals and associated work copy images captured under this legislation.
[insert your answer here]	
IM12	It is mandatory that thumbnails are at 100w by 125h pixels and are stored in the Image Repository compressed using JPEG Sequential Baseline mode to a target size of between 4KB and 5KB. Number of resolution levels: The image shall be encoded using enough resolution levels to ensure that a thumbnail with max (width, height) <= 64 is available in the image. Example: a 640x480 image shall be encoded with 5 resolution levels, which enables sub-resolution decodes of 320x240, 160x120, 125x100 and 80x60.
[insert your answer here]	
IM13	It is mandatory that the system(s) incorporate(s) the ability to categorise images into logically partitioned repositories for the storage of images according to their category. (Formal, Missing Persons, Firearms Licence Holders, Suspect etc)
[insert your answer here]	
IM14	It is mandatory that the system(s) can import image(s) regardless of source. This includes, but is not limited to, images from the following sources: (i) Livescan/ABIS (ii) Digital cameras (iii) iPhone (iv) Still capture of frames from both analogue and digital video sources (eg CCTV and video camera footage) (v) Images produced by composite likeness software (vi) Scanning of any hard copy photograph, slide or negative (eg forged identification documents or developed 35mm film) (vii) Any other recognised industry standard image software format (eg BMP, JPEG, TIFF, PNG, etc). (viii) External interface/source system
[insert your answer here]	

IM15	It is mandatory that the system retains meta data for a Formal Photo. This information should include, but is not limited to: (i) Image Identifier (unique) (ii) Image Type (List) (iii) Photographing Officer Name (iv) Photographing Officer ID (v) Date Photo Taken (vi) Time Photo Taken (vii) Date Photo Entered (viii) Station where photo taken (ix) NIA Person ID and/or PRN
[insert your answer here]	
IM16	It is mandatory that the system retains meta data for a Formal Photo. This information should include, but is not limited to: (x) NIA (DocLoc) Case Number (xi) Image Identifier (unique) (xii) Image Type (List) (xiii) Photographing Officer Name (xiv) Photographing Officer ID (xv) Date Photo Taken (xvi) Time Photo Taken (xvii) Date Photo Entered (xviii) Station where photo taken (xix) Offence Type (List) (xx) TCN (xxi) NIA Person ID and/or PRN (xxii) Driver Licence Number
[insert your answer here]	
IM17	It is mandatory that the system retain meta data for a suspect image. This information should include, but is not limited to: (i) NIA (DocLoc) Case Number (ii) NIA Person ID (iii) Suspect Image Identifier Number (unique) (iv) Image Type (List) (v) Photographing Officer Name (vi) Photographing Officer ID (vii) Date Entered (viii) Station (where image captured) (ix) Offence Type (List) (x) Image enrolled by QID
[insert your answer here]	
IM18	It is desirable that suspect images may have a 'Time to Live' allocated. Once the Time to Live period has expired the images will be omitted from searches unless specifically requested.
[insert your answer here]	

IM19	It is desirable that the Time to Live parameter is configurable per suspect image but has an initial default value.
[insert your answer here]	
IM20	It is mandatory that when a suspect image is matched and positively identified then the system(s) provide(s) a function to receive the NIA recorded name and update the suspect record meta data.
[insert your answer here]	
IM21	It is mandatory that the system retain meta data for a Firearms Licence image. This information should include, but is not limited to: (i) NIA Firearms Case Number (sourced from NIA) (ii) Image Identifier (Unique) (iii) Firearms Licence Number (FLICNO) (sourced from NIA) (iv) Image Type (List) (v) Likeness Verification Officer's Name (vi) Likeness Verification Officer's ID (vii) Date Entered (viii) Station (Nearest Arms Office to the licence holders residence) (ix) Licence Type (sourced from NIA) (Multi Select List [as a dealer must also have a standard licence]) (A = Standard, D = Dealer) (x) Endorsement Type (sourced from NIA) (List of 9 and must be multi-select) (B = Pistol, C Collector/general, C Heirloom, C Memento, C Theatrical, C Museum, C Kea Gun, E = Military Style Semi-Automatic, F = Dealer) (xi) Licence Expiry Date (sourced from NIA) (xii) Licence Holder Postal Address (sourced from NIA)
[insert your answer here]	
IM22	It is mandatory that the system retain meta data for a missing person image. This information should include, but is not limited to: (i) NIA (DocLoc) Case Number (ii) Missing Person image Identifier (unique) (iii) NIA Person ID (iv) Image Type (List - include Other for medical images such as dental records) (v) Capture Officer's Name (vi) Capture Officer's ID (vii) Date Photo Taken (year) (viii) Date Image Entered (ix) Station Image Entered (x) Missing Category (NIA) (xi) Status (NIA Located field)
[insert your answer here]	
IM23	It is mandatory that Formal photo images must include a permanent retention indicator. This indicator is set & removed based on NIA details. The indicator may set when an image is imported or triggered by receipt of an interface transaction.

[insert your answer here]	
IM24	It is mandatory that an individual within IMS can have their information sealed by an authorised user.
[insert your answer here]	
IM25	It is mandatory that a Sealed Identity can be only be viewed or returned in a search result (recognition or metadata) by an authorised user.
[insert your answer here]	
IM26	It is desirable that one or more selected photos for an individual are available for import and enrol against a new identity.
[insert your answer here]	

5.4 Image –Import of non Livescan/ABIS

ID	DETAIL
IN1	It is mandatory that the system(s) provides an interface to import digital images from media sources.
[insert your answer here]	
IN2	It is mandatory that the system(s) provides an interface to acquire and scan images from TWAIN compliant sources such as Flat Bed Scanners.
[insert your answer here]	
IN3	It is mandatory that the system provide an interface to import digital images from a system folder.
[insert your answer here]	
IN4	It is mandatory that the system(s) has/have the ability to import and enhance both: (i) Black and white photographic images (ii) Colour photographic images
[insert your answer here]	
IN5	It is mandatory that the system(s) has/have the ability to execute the following steps within the Import process: (i) View images for quality assurance / quality control purposes (ii) Run a biometric search of existing repositories (iii) Source metadata from core NZP applications (iv) Classify SMTs within current operation (Police Structure) (v) Return metadata updates to the core NZP applications when required (vi) Create a thumbnail image (vii) Store image(s), including the original and working copies.
[insert your answer here]	

IN6	It is desirable that the system(s) has/have the ability to execute the following steps within the Import process: (i) Classify Clothing, logos and /or patterns within current operation (Police Structure)
[insert your answer here]	
IN7	It is mandatory that the system facilitates the import of working copy(ies) of facial frontal images in accordance with the ANSI/NIST Best Practice Recommendations by: (i) Assisting the user with centring and sizing the image correctly (with on-screen visual guidelines including crop and rotate capabilities) (ii) Providing a real time image preview in cropped ANSI/NIST compliant view layout (iii) Following import (and automatically cropping, if necessary) of the image with an aspect ratio of 1:1.25 for facial images. (iv) Following different formats to accommodate associated images and metadata.
[insert your answer here]	
IN8	It is mandatory that the system(s) has/have the ability to enhance/adjust working copy images during the import process and prior to permanent storage by: (i) Converting to grey scale (ii) Enhancing pixel by pixel (iii) Adjusting colour, colour saturation, colour hue. (iv) Size (v) Brightness (vi) Colour correction including red-eye (vii) Cropping for subject (viii) Orientation
[insert your answer here]	

5.5 Image – Input NIST from Livescan/ABIS

Livescan/ABIS capture biometric details within NIST file. Each of these files is made up the following:

(i) One ANSI/NIST Type-1 Transaction Information record

(ii) One ANSI/NIST Type-2 user-defined descriptive text record containing key charge meta-data (e.g. TCN) and other data required

(iii) One (or more if multiple images) can be captured per charge ANSI/NIST Type-10 facial & SMT image record, containing image meta-data and the JPEG compressed image as part of a JFIF file.

ID	DETAIL

IL1	It is mandatory that the system(s) provides an interface to import file(s) from Livescan/ABIS. Images are embedded within a NIST file. A NIST file may contain multiple images related to a Formal Photo. Livescan/ABIS provide a TCN Number as the unique reference.
[insert your answer here]	
IL2	It is mandatory that the system(s) has/have the ability to execute the following steps for the original image within the Import process: (i) View images for quality assurance / quality control purposes (ii) Source metadata embedded within or associated to the imported NIST file (iii) Run a biometric search of existing repositories (iv) Source metadata from core NZP applications (v) Classify SMTs within current operation (Police Structure) (vi) Return metadata updates to the core NZP applications when required (vii) Create a thumbnail image (viii) Store image(s), including the original and working copies.
[insert your answer here]	
IL3	It is desirable that the system(s) has/have the ability to execute the following steps for the original image within the Import process: (i) Classify Clothing logo and/or patterns within current operation (Police Structure)
[insert your answer here]	
IL4	It is mandatory that the image management system facilitates the use of working copy images in accordance with the ANSI/NIST Best Practice Recommendations by: (i) Assisting the user with centring and sizing the image correctly (with on-screen visual guidelines and pan, tilt, rotation and zoom capabilities) (ii) Providing a real time image preview in cropped ANSI/NIST compliant view layout (iii) Following import (and automatically cropping, if necessary) of the image with an aspect ratio of 1:1.25 for facial images (iv) Following different formats to accommodate images and associated metadata.
[insert your answer here]	

IL5	It is mandatory that the system(s) has/have the ability to enhance/adjust working copy images during the import process and prior to permanent storage by: (i) Converting to grey scale (ii) Enhancing pixel by pixel (iii) Adjusting colour, colour saturation, colour hue (iv) Size (v) Brightness (vi) Colour correction including red-eye (vii) Cropping for subject (viii) Orientation.
[insert your answer here]	

5.6 Biometric – Enrolment and Matching

ID	DETAIL
BE1	It is mandatory that the user can select any image retrieved by the biometric matching process and display all the details (both associated images and metadata) stored in any image repository for recognition search.
[insert your answer here]	
BE2	It is desirable that the user has the ability to control the number of images that are retrieved as the result of the biometric matching process within a configurable range for recognition search.
[insert your answer here]	
BE3	It is mandatory that the most likely matches are presented to the user ranked in descending order of match likelihood using an intuitive measure of confidence rating, which must show for recognition search.
[insert your answer here]	
BE4	It is mandatory that recognition matching can be performed across all compliant image repositories.
[insert your answer here]	
BE5	It is mandatory that an intuitive and easily operable manual or automated anchoring process be provided to ensure that the biometric algorithm is correctly applied to the image that is the subject of the enrolment, matching or search.
[insert your answer here]	
BE6	It is mandatory that the facial recognition matching can be performed for any newly acquired image, or previously enrolled image, against any image repository or repositories on an ad-hoc basis using a recognised and proven biometric algorithm.
[insert your answer here]	
BE7	It is mandatory that the facial recognition matching that is performed for any newly acquired image or previously enrolled image against any image repository or repositories is able to be done on a rules based method.

[insert your answer here]	
BE8	It is desirable that the SMT recognition matching can be performed for any newly acquired image, or previously enrolled image, against any image repository or repositories on an ad-hoc basis using a recognised and proven biometric algorithm.
[insert your answer here]	
BE9	It is desirable that the clothing symbol/pattern recognition matching can be performed for any newly acquired image, or previously enrolled image, against any image repository or repositories on an ad-hoc basis using a recognised and proven biometric algorithm.
[insert your answer here]	

5.7 Biometric – Auto Match on enrolment

ID	DETAIL
BA1	It is mandatory that the system(s) will perform automated matching of new images at the time enrolment against images stored in the Image repositories (rules apply) and watch list mechanism.
[insert your answer here]	

The following table describes the rules associated with BA1 above.

Repository		Auto match on enrolment
Formal Photos	Offender	All Repositories
	CPOR	All Repositories
	Returned Offenders	All Repositories
Voluntary		Offender, Suspect and Missing Person
Firearms Licence		All Repositories
Suspect		All Repositories
Missing Person		All Repositories

5.8 Watch List

ID	DETAIL
WL1	It is mandatory that the system(s) provide(s) for real-time watch list monitoring.
[insert your answer here]	
WL2	It is mandatory that the system(s) provide(s) the ability for an approved user to maintain a variable number of discrete watch lists
[insert your answer here]	
WL3	It is mandatory that when a match occurs on watch list image and a newly enrolled image, then a notification will be sent to the enrolling user and to the watch list entry requestor.
[insert your answer here]	
WL4	It is mandatory that an approved user may view a watch list.

[insert your answer here]	
WL5	It is mandatory that an approved user may remove a watch list, or watch list entry.
[insert your answer here]	
WL6	It is mandatory that all images added to a watch list have a 'Time to Live' associated with the watch list entry after which time the entry is automatically removed from the watch list.
[insert your answer here]	
WL7	It would be desirable that the Time to Live parameter is configurable per watch list entry but has an initial default value.
[insert your answer here]	
WL8	It is desirable that the threshold level for automated matching is configurable by image type.
[insert your answer here]	
WL9	When a new enrolling image is matched to a Missing Person image and positively identify then the system provides a function to notify the user enrolling the new image.
[insert your answer here]	

5.9 Firearms Licence update & card production

Production of a physical firearm licence cards occurs weekly and involves the following process steps:

1. NIA extract Firearms Licence data for licences that are to be produced.
2. Photo Manager / Image Management System imports the file.. For each licence that NIA has identified, the user visually verifies the IMS Firearms details against those from NIA. Verified licence details and images are extracted for card production.
3. Licence and images are transferred to the card provider (ABCorp).
4. IMS records the date/time the licence was extract to the card provider.

ID	DETAIL
FL1	It is mandatory that the system provide a process to receive licence details from NIA.
[insert your answer here]	
FL2	It is mandatory that the user verify the system(s) details for the Firearms against those imported from NIA.
[insert your answer here]	
FL3	It is mandatory that the Image for the licence card is extracted to the prescribed folder structure.
[insert your answer here]	
FL4	It is mandatory that the meta-data for card production is extracted to file in the format prescribed by the card provider. Currently this is a text file.
[insert your answer here]	

FL5	It is mandatory that the meta-data extract and images are transferred to the card provider.
[insert your answer here]	
FL6	It is mandatory that the system(s) produce a control report for the licence card production process.
[insert your answer here]	

5.10 Queries

ID	DETAIL
SR1	It is mandatory that the system(s) provide(s) the capability to carry out quality assurance/quality control images and metadata. Quality assurance is based on quality score for an enrolled image(s). The details may be searched/filtered by user, Station (location) and time period.
[insert your answer here]	
SR2	It is mandatory that searching can be conducted dynamically in real time using multiple fields.
[insert your answer here]	
SR3	It is mandatory that the user can select any record retrieved by the searching process and display all the details (both other images and metadata) stored on any of the system(s) repositories relating to that image(s).
[insert your answer here]	
SR4	It is mandatory that the system(s) provide(s) the capability to search and retrieve enrolled images based on metadata using text-based searches in conjunction with biometric, SMT and pattern recognition. The Respondent is to describe the search capabilities of the solution.
[insert your answer here]	
SR5	Common Search Criteria for all image database will include, but are not limited to the following fields: (i) NIA (DocLoc) Case Number (ii) Image Identifier (unique) (iii) TCN Number (LiveScan/ABIS) (iv) Name (First, Middle, Last) (v) NIA Person ID Number (vi) PRN (from NIA) (vii) Date of Birth (DOB) and Date Range (viii) Gender (ix) Age and Age Range (x) Height and Height Range (xi) Eye Colour with multiple selection (xii) Glasses (xiii) Hair Colour with multiple selection (xiv) Hair type (style) (xv) Hair length

	(xvi) Facial hair (xvii) Build with multiple selection (xviii) Ethnicity with multiple selection (xix) Photo Reference Number (data migrated from IMS) (xx) Image Category (List) (xxi) Date Photo Entered (xxii) Station where photo taken (xxiii) Optionally, any other Image management system search fields (xxiv) Offence Type with multiple selection (xxv) Charge Station with multiple selection (xxvi) Arrest Record (xxvii) Arrest Date and Date Range (xxviii) QID Livescan User or person capturing the image (xxix) Date image captured (xxx) Date image record modified (with details) (xxxi) Include expired suspect time to live images.
[insert your answer here]	
SR6	It is desirable that the user has the ability to control the number of images that are retrieved as a result of the searching process so that only images that match above a configurable matching threshold are displayed.
[insert your answer here]	
SR7	Common result set for search for all image databases should include but is not limited to the following fields: (i) Image set(s) (ii) Name (First, Middle, Last) (iii) Arrest Date (iv) TCN (v) Gender (vi) Ethnicity (vii) Age (viii) Date of Birth (DOB) (ix) Photo Reference Number (IMS) (x) PRN (xi) NIA Person ID Number.
[insert your answer here]	
SR8	It is desirable that the system(s) Results Set is returned with the best match first.
[insert your answer here]	
SR9	It is desirable that the system(s) initially group(s) all records for each person together in the Results Set and presents all previous records for the same person in reverse chronological order.
[insert your answer here]	

SR10	It is mandatory that one or more of the search results may be included in predefined output. Eg Flyer, photo book`
[insert your answer here]	

5.11 Flyer

ID	DETAIL
FY1	It is mandatory that the user can either print, or store as a secured Adobe ® PDF file, a 'flyer' for any selected image(s). Content is based on the configurable template(s).
[insert your answer here]	
FY2	It is desirable that the user can also enter information in a free-text field to be displayed on the flyer to detail the Reason for Interest in the person(s). This can be associated to an image or to the overall page.
[insert your answer here]	
FY3	It is mandatory that template(s) for one page flyer can be configured by an authorised user.
[insert your answer here]	

5.12 Photo Line-Up

A line up is a group of images (displayed on a single page) used to conduct a formal photo identification. The candidate for a Photo Line Up must be a specific and known individual.

At least 7 other photos along with the candidate image are shown to a witness with the Candidate's (suspect) image randomly placed. It must be placed differently for each witness and not be in first place. No names or means of identification must be shown to the witness.

Where the line-up includes a Police employee as a witness, at least 9 other photos along with the suspect image are shown to the witness.

The number of photos in a line-up can be varied between 8 and 20 in increments of 2.

ID	DETAIL
LP1	It is mandatory that a Photo Line-up contains Facial images only.
[insert your answer here]	
LP2	It is mandatory that a Photo Line-up production can be undertaken by any authorised user.
[insert your answer here]	
LP3	It is mandatory that the system(s) provide(s) the capability to create printed and electronic photo line-ups that are easy to present to witnesses in a printed format and electronic, and suitable for evidential purposes.
[insert your answer here]	
LP4	It is mandatory that any witness interaction with a prepared electronic photo line-ups, including the witness details and any selections made must be recorded

[insert your answer here]	
LP5	It is mandatory that the creation of a photo line-up can be initiated using an image retrieved from the Formal photo repository or sourced though any image acquisition This image is the Candidate photo.
[insert your answer here]	
LP6	It is mandatory that the eligibility for filler images be verified prior to use in a Photo Line Up. Eligibility for filler images: (i) Status check against core NZP systems (ii) Sourced from Formal photo repository and subject to Permanent Retention.
[insert your answer here]	
LP7	It is mandatory that all the images presented to the user as filler candidate for inclusion in a Photo Line-up are able to be retrieved from the Formal photo repository using physical attribute matching in conjunction with textual-based searching.
[insert your answer here]	
LP8	It is desirable that the user can select that all the images presented to the user as a filler for inclusion in a Photo Line-up are able to be retrieved from the Formal photo repository using the system's biometric facial recognition in conjunction with attribute matching and textual-based searching.
[insert your answer here]	
LP9	It is mandatory that the number of images in each created line-up be from a minimum of 8 photos to a maximum of 20 photos.
[insert your answer here]	
LP10	It is mandatory that the number of photos in a line-up be variable between 8 and 20 in increments of 2 (i.e. 14, 16, and 18).
[insert your answer here]	
LP11	It is mandatory that each line-up will have a unique automatically generated Line-up Reference Number
[insert your answer here]	
LP12	It is mandatory that the system prevent a user form including two images of the same person (NIA Person ID) within a Photo Line-up.
[insert your answer here]	
LP13	It is mandatory that the candidate photo of the line-up can be accommodated into the line-up in a random position amongst all the selected candidate filler images from the Formal photo repository.
[insert your answer here]	
LP14	It is mandatory that the candidate photo of the line-up cannot be placed in the first place in the line-up.
[insert your answer here]	

LP15	It is mandatory that the completed photo line-ups are able to be exported (produced) for witness viewing. Note the following preferred NZ Police export formats and media: (i) an electronic presentation template containing defined preamble slides and a single appropriately sized image per slide (ii) an electronic Photo Line Up stored as a secured Adobe ® PDF file comprising all images appropriately sized and spaced to fit neatly on A4 sheets (or A3 sheets) without any empty image slots
[insert your answer here]	
LP16	It is mandatory that when any line-up is produced that both a witness and police copy must be created together and be distinguishable by electronic filename and by Page Title.
[insert your answer here]	
LP17	It is mandatory that the line-up produced for witness viewing only has the sequence number of the image within the line-up clearly displayed against each image. In the case of electronic templates the line-ups must also contain the prescribed preamble slides, which must be maintainable by an authorised user.
[insert your answer here]	
LP18	It is mandatory that a copy for internal police use must always be produced in the one page Photo Line Up regardless of the format of the witness copy.
[insert your answer here]	
LP19	It is mandatory that the following Person related information from the Formal photo repository is clearly displayed under each image on the line-up for internal police use and Line-up related information is recorded and saved with each line-up: Person related detail: (i) Last Names, Givens names. (ii) NIA Person ID number (iii) Age (iv) Unique Image Reference Number (v) Photo capture date Line-up related detail: (vi) (DocLoc) Case Number (Optional) (vii) Requesting Officer's Name (Optional) (viii) Requesting Officer's ID (Optional) (ix) Creating member Name (x) Creating Member ID (xi) Date
[insert your answer here]	
LP20	It is mandatory that if the candidate image used for the line-up has been externally acquired, then the displayed metadata is enterable for use on the internal police copy.
[insert your answer here]	

LP21	It is mandatory that the system allows enhancement to any image within a line-up.
[insert your answer here]	
LP22	It is mandatory that any completed line-up can be saved to a central repository and can be re-opened for further line-up viewing or printing but cannot be modified.
[insert your answer here]	
LP23	It is mandatory that a completed and saved line-up can be used as the basis to create a new one with the candidate photo in a different place than the original saved line-up (re-shuffle). The user can request a number of different line-up versions up to a maximum of 7 that will result in this number of distinct randomly ordered line-ups being produced in which the candidate image is always positioned in a different place in each line-up for display to different witnesses. The production of each line-up can be recorded along with the position in which the candidate image was displayed. This would allow subsequent requests to produce further versions of a line-up to place the candidate image in a different position to any previous line-up version produced.
[insert your answer here]	
LP24	It is mandatory that the number of images retrieved and available for inclusion in the line-up is displayed to the user.
[insert your answer here]	
LP25	It is desirable that the creation of a photo line-up can be performed using intuitive single mouse click and keyboard controls such as the dragging and dropping of images selected for inclusion into the line-up.
[insert your answer here]	
LP26	It is mandatory that the candidate of the line-up is clearly displayed to the user at all times whilst filler images are being selected for inclusion in the line-up.
[insert your answer here]	
LP27	It is mandatory that the population of the electronic template is automated such that all the selected images are inserted into their corresponding locations in the template and the User has the ability to resize the image and use 'enhancement tools' including background change capability if required.
[insert your answer here]	
LP28	It is mandatory that the population of the electronic Photo Line Up is automated such that all the selected images are inserted into their corresponding locations on the sheet and the images are automatically spaced and sized
[insert your answer here]	

5.13 Photo Book

This function is the ability to create a collection of images based upon selected criteria. Identifying details for each subject in the photobook must be displayed.

Such a Photo Book may be all members of a particular gang; or all burglars or paedophiles in a particular area; or all Firearms Licence Holders in a particular town; or all Missing Persons in a Police District.

NZP do not use photo books for witness viewing.

ID	DETAIL

PB1	It is mandatory that the system provide the capability to create a printed photo book.
[insert your answer here]	
PB2	It is desirable that the system provide the capability to create an electronic photo book.
[insert your answer here]	
PB3	It is mandatory that the system(s) provide(s) the capability to create a title for each photo book.
[insert your answer here]	
PB4	It is mandatory that all the images presented to the user as individual as for inclusion in a photo book are retrieved from multiple databases in the system(s), using the systems' textual-based searching facilities and biometric/pattern matching.
[insert your answer here]	
PB5	It is mandatory that the images to be retrieved can be controllable by the user.
[insert your answer here]	
PB6	It is desirable that the population of the electronic template is automated such that all the selected images are inserted into their corresponding locations in the template and the images are automatically spaced and sized.
[insert your answer here]	
PB7	It is mandatory that once saved, the electronic Photo Book can be reopened, reviewed and may be printed by authorised users.
[insert your answer here]	
PB8	It is desirable that an electronic photo book can be copied and edited to create a new photobook.
[insert your answer here]	
PB9	It is mandatory that a partially completed photo books can be saved in draft format.
[insert your answer here]	
PB10	It is mandatory that the Images resulting from different search criteria retrievals can be used to complete the population of a photo book.
[insert your answer here]	
PB11	It is mandatory that each image will also display/print the individual's details.
[insert your answer here]	

5.14 Investigative Features

ID	DETAIL
IV1	NZ Police currently use FACES version 4 from IQ Biometrics to create composite likenesses of suspects and offenders. It is mandatory that the system must be able to import images that have been output from FACES, and use these as probe image in a recognition search.
[insert your answer here]	

IV2	It is mandatory that the system(s) provide(s) the capability for a user to view all images of a particular person, including historical images, and allow for all images to be selected and viewed, and printed.
[insert your answer here]	
IV3	It is mandatory that the system(s) must provide image enhancement capabilities for all types of image regardless of source.
[insert your answer here]	
IV4	It is mandatory that the system(s) must include(s) the ability to add or remove features such as facial hair, jewellery, glasses, scars, etc to assist in determining the likely current appearance of an individual
[insert your answer here]	
IV5	It is mandatory that the system(s) include(s) the ability to enhance poor quality images by sharpening details and zooming into areas on interest to assist with criminal investigations
[insert your answer here]	
IV6	It is mandatory that the system(s) include(s) the ability to accommodate receipt of image formats from a wide variety of industry sources (such as those that require Multiplex Drivers, those that require Codec software, MPEG, AVI files etc) and allows captured still images or frames to be loaded as JPEG files.
[insert your answer here]	

5.15 Reporting

ID	DETAIL
RP1	It is desirable that the system(s) is able to export data to Police's corporate reporting tool (SAS).
[insert your answer here]	
RP2	It is mandatory that the system(s) provide management reporting. This may include but is not limited to: (i) Count of Image enrolment (ii) Counts of Photo books produced (iii) Counts of Photo Line Up production (iv) Counts of recognition searches conducted, by type (v) Count of Firearms Licence card productions actioned (vi) User activity statistics (vii) Count of watch list hits Reports may be filtered/broken down by time period, NZ Police district/area/station, User who actioned, requesting user, result of line-up.
[insert your answer here]	
RP3	It is mandatory that the system(s) provide operational reporting. This may include but is not limited to: (i) Report of Image enrolment (ii) Report of Photo books produced (iii) Report of Line up production, including date shown to witness and if witness selected a candidate.

	(iv) Report of recognition searches conducted, including intelligence link. (v) Report of recognition search hit rates. (vi) Report of watch list. (vii) Error reporting, any images that could not be loaded. Reports may be filtered/broken down by time period, NZ Police district/area/station, User who actioned, requesting user, repository, image type
[insert your answer here]	
RP4	It is desirable that a user can create, customise, save and share a report / output. The Respondent is to describe how the solution supports users defining and running reports to meet their needs.
[insert your answer here]	

6 NON FUNCTIONAL

6.1 Performance

Category	Historic Records (Current)	Estimated Additional Records per Annum (Future)	Estimated Transactions Volumes	Desired Response Times
Image Management - Formal	1.5m from 800,000 individuals	50,000 per annum	Current Image retrieval requests from NZP core applications 60,000 per day. Note the **'Loads"** volume is the same as the **'additional** records, if previous column.	The retrieval of a thumbnail or full image to a NZP core application be returned within 100 milli seconds for 95 % of the requests (10 per second). The retrieval of a full set of thumbnails to a NZP core application be returned within 200 milli seconds for 95% of the requests (5 per second). It is desirable that an image can be loaded within 30 seconds. This would see minimal user interaction to complete the load. The steps to loading an image are: (i) View images for quality assurance / quality control purposes (ii) Run a biometric search of existing repositories (iii) Source metadata from core NZP applications (iv) Classify SMTs within current operation (Police Structure) (v) Return metadata updates to the core NZP applications when required (vi) Create a thumbnail image (vii) Store image(s), including the original and working copies. Solution response times for steps (i), (ii), (vi) and
Image Management - Suspect	N/A	7,500 per annum		
Image Management - Firearms Licence holders	245,000 at any one time	10,000 renewals per annum 9,500 new per annum 9,500 removed per annum.		
Image Management - Missing Persons	200	500 per annum		
Image Management – Child Protection (Child Sex Offender Register)	1,500	2,300 per annum		

Category	Historic Records (Current)	Estimated Additional Records per Annum (Future)	Estimated Transactions Volumes	Desired Response Times
				(vii) to be completed within 5 seconds (for each step).
Facial Recognition Search, Compare, Match and Report Excluding image load process.	Nil	At least 15,000 per annum	At least 15,000 per annum	All Search, Compare, Match, and Report transactions (including using multiple metadata fields) be completed within 5 seconds.
Photo line-up Production	12,000 (Time to prepare: 20 – 60 minutes)	15,000 per annum (Time to prepare: 10 minutes)	15,000 per annum	Solution response times for production of a Photo Line Up with no user selection (ie initial display of images) be completed within 5 seconds.
Scars Marks and Tattoos / Clothing Logos	Nil	30,000 (estimated)	30,000 (estimated)	All Search, Compare, Match, and Report transactions (including using multiple metadata fields) be completed within 5 seconds.

Notes:

1. These Records exclude capture of additional images which will arise from inter agency Identity Management work (Drivers licences, passports, etc.).
2. These Records are based on existing Police Processes, legislation changes will see future substantial increases

ID	DETAIL
NFP1	It is mandatory that the solution support 70 concurrent users located though out New Zealand.
[insert your answer here]	
NFP2	It is mandatory that the Respondent outline how they will support the performance requirements specified in the above table.
[insert your answer here]	
NFP3	It is mandatory that the Respondent outline what is required to scale the solution by: (i) Doubling (above numbers x 2) (ii) Tenfold (above numbers x 10).
[insert your answer here]	

NFP4	The Respondent is to provide the facial recognition and pattern search response times for their solution.
[insert your answer here]	
NFP5	The Respondent is to provide the response times for their solution for production of a Photo Line Up with no user selection (ie initial display of images).
[insert your answer here]	
NFP6	The Respondent is to provide the response times of their solution for biometric Searches on: (i) Facial frontal images (ii) SMT pattern matching.
[insert your answer here]	
NFP7	It is mandatory that patching must be managed in accordance with NZISM. https://www.gcsb.govt.nz/publications/the-nz-information-security-manual
[insert your answer here]	
NFP8	It is mandatory that, all images and metadata NOT subject to destruction in IM11 are retained permanently.
[insert your answer here]	
NFP9	It is mandatory that, unless deleted by an authorised user, the following data is retained permanently: (i) Images and associated meta-data (ii) Photo Line Ups (iii) Photo books
[insert your answer here]	
NFP10	It is mandatory that User Activity Logs be retained permanently.
[insert your answer here]	

6.2 Usability

Requirements that ensure the appearance of the solution conforms to the expectations of NZP organisation and its users.

ID	DETAIL
NFU1	The Respondent shall describe the user interface of the major components of their solution.
[insert your answer here]	
NFU2	It is desirable that the systems should be designed to minimise the number of screen interactions, key presses and clicks required by the User to perform the critical processes supported by the System.
[insert your answer here]	

NFU3	It is desirable that the user interface will use terminology that is consistent with the NZP core operational data set.
[insert your answer here]	
NFU4	It is desirable that the format of information will be consistent with NZP core operational data set. eg DOCLOC Case Number, 10 digit numeric is formatted nnnnnn/nnnn
[insert your answer here]	
NFU5	It is mandatory that the user interface will use NZ format date/time.
[insert your answer here]	
NFU6	It is mandatory that the documents will use NZ format date/time.
[insert your answer here]	
NFU7	It is mandatory that documents produced may include confidentiality or disclosure statement where specified. The content of the station must be configurable. Current statement is: "This document is distributed in confidence to members of New Zealand Police. Possession of this document without lawful authority or excuse is an offence against Section 61(A) of the Policing Act 1958."
[insert your answer here]	
NFU8	It is mandatory that documents produced may include Police branding, including headings and logo where specified.
[insert your answer here]	
NFU9	It is desirable that documents will use terminology that is consistent with the NZP core operational data set for headings and field labels.
[insert your answer here]	
NFU10	It is desirable that the user interface behaviour within the systems are to have standard Windows alternative keyboard shortcuts provided. Eg Tab between fields, tab on auto complete, Ctrl-S is save.
[insert your answer here]	
NFU11	It is desirable that the user interface support touch screen users.
[insert your answer here]	
NFU12	It is desirable that messages can be configured to be meaningful to NZP process and terminology.
[insert your answer here]	
NFU13	It is desirable that errors, warnings displayed to user must be in plain language and indicate appropriate action to be taken.
[insert your answer here]	

6.3 Product & User Environment

Requirements for the physical environment within which the solution will operate.

ID	DETAIL
NFE1	Users within the enterprise environment are geographically dispersed throughout the NZ
[insert your answer here]	
NFE2	Users of the Image Management features are based within the National Biometric Information office.
[insert your answer here]	
NFE3	Users of the Case Investigation features are located though out the country.
[insert your answer here]	
NFE4	It is mandatory that all NZP user access all solution components via the NZP enterprise network or NZP mobility network.
[insert your answer here]	
NFE5	NZP Users may access the NZP enterprise environment via remote access tools. Network support levels vary greatly depending on the user's actually physical location.
[insert your answer here]	
NFE6	User access to USB ports, DVD and external media is restricted. Permission is granted to a user via an established NZP process. It is mandatory that the solution does not assume that a user has access to an external media device.
[insert your answer here]	
NFE7	Users may access a folder(s) to load images that have been emailed, scanned or transferred for importing into the solution. Permission for folder address is granted to a user via an established NZP process. It is mandatory that the user will choose the folder(s) for saving or retrieving files (images, documents etc.).
[insert your answer here]	
NFE8	Users work on a managed desktop. The ability to manage, configure or install software the on a workstation is restricted. It is mandatory that the desktop components must be configured and packaged for installation via the established NZP distribution process.
[insert your answer here]	
NFE9	It is desirable that the solution should operate correctly where the (workstation) logged on user has no local admin or install privileges.
[insert your answer here]	
NFE10	It is mandatory that the application is used on Windows 8.1 and Windows 10 workstation, laptop or tablet.
[insert your answer here]	
NFE11	It is mandatory that the Web based application components must be compatible with IE11 and CHROME v54 – and subsequent product releases.
[insert your answer here]	

NFE12	It is desirable that data must be retained within NZ.
[insert your answer here]	
NFE13	It is mandatory that DR and production solution must be geographically dispersed.
[insert your answer here]	
NFE14	The solution design will be submitted to NZP design review process (TAG & TCF). The vendor will work with the NZP ICT Technical Owner to complete the necessary high level & detailed design. Note: Should part of or the whole solution see data retained outside of NZ, the complexity of gaining approvals and "Certificate and Accreditation" is greater.
[insert your answer here]	

6.4 Data & Image Format

ID	DETAIL
NFF1	The Respondent shall describe the image formats used during the load, storage and transmission of the images by and within the solution, and for the long term evidential storage including the following: (i) Whether the image format is proprietary or a widely supported standard format. (ii) Whether the image format uses lossless compression or lossy compression. (iii) What software is required to view, resize, export, compress or convert the images into a standard image format, such that: (1) The image can be viewed on a standard Police end user device without requiring the installation of any additional or specialised software. (2) The image conforms to the NZ e-GIF standard. (IV) Whether the image format incorporates any digital watermark mechanism that can be used to verify the image has not been subsequently tampered after capture.
[insert your answer here]	
NFF2	The Respondent shall provide minimum, maximum and recommended resolution digital images the solution is capable of capturing. (i) For each resolution include the number of pixels as width, height, and total number of megapixels (MP or Mpx) (ii) For each resolution provide an indication of the corresponding digital image file size (MB) in the image format native to the solution. (iii) For each resolution provide an indication of the corresponding digital image file size (MB) in the JPG image format (if different to the native format).
[insert your answer here]	
NFF3	The Respondent shall describe any secure long term storage options available or supported by the solution for retention of data and images form a period of seven (7) years while preserving the evidential trail.
[insert your answer here]	

6.5 Licensed Software

ID	DETAIL

NFL1	The Respondent shall describe how the solution (including software, hardware and services) will be licenced to NZ Police. The Respondent shall provide the following information: (i) Who owns any licenced components of the solution? (ii) If the Respondent is not the owner, the Respondent's interest and rights in the licenced components of the solution (e.g. exclusive distributor, accredited reseller/installer/support service provider etc.). (iii) Restrictions applied to the licenced component of the solution that will restrict or preclude NZ Police form having the software operated, supported, enhanced, modified or upgraded by. (1) NZ Police itself or (2) Any third party (eg an existing or future contractor of NZ Police). (iv) Escrow. It is desirable that the Respondent agree to NZ Police's access to, and free usage of, commercial solution if one of the following events occurs: (1) Company files for bankruptcy or ceases to operate (2) Software becomes unsupported without an upgrade path. (v) Identify any solutions features that have a licence cost
[insert your answer here]	

6.6 Availability and Hours of Operation

Quantifies the necessary reliability of the solution and defines the expected hours of operation.

Terms:

- System failure – an outage or a fault with a severity that prevents the users form using the system in an operational capacity.

ID	DETAIL
NFH1	It is mandatory that images must be available to NZP operational applications seven days a week, 24 hours a day subject to agreed outages.
[insert your answer here]	
NFH2	It is mandatory that Facial Recognition features are available seven days a week, 24 hours a day subject to agreed outages.
[insert your answer here]	
NFH3	It is mandatory that SMT Recognition features are available seven days a week, 24 hours a day subject to agreed outages.
[insert your answer here]	
NFH4	It is mandatory that Case Investigation features must be available seven days a week, 24 hours a day subject to agreed outages.
[insert your answer here]	
NFH5	It is mandatory that Image Capture is available seven days a week, 24 hours a day subject to agreed outages
[insert your answer here]	
NFH6	It is mandatory that Query, View, Search using metadata and/or biometric criteria must be available seven days a week, 24 hours a day subject to agreed outages

[insert your answer here]	
NFH7	It is mandatory that the system is to be available 99.9% outside of the agreed outage window(s). 99.9% equates to 86.4 seconds a day, or 43 minutes a month or 8.77 hours a year.
[insert your answer here]	
NFH8	Routine outages must be scheduled between Sunday 06:00 and 08:00 NZ time.
[insert your answer here]	
NFH9	Following recovery, it is mandatory the maximum loss of data after recovery from a disaster (RPO) is not more than 4 hours.
[insert your answer here]	
NFH10	In the event of a system failure, it is mandatory that the system is restored within required recovery time after a disaster (RTO) for the solution of 8.77 hours.
[insert your answer here]	
NFH11	It is mandatory that recovery occurrences must not exceed 1 in any consecutive 12 month period.
[insert your answer here]	
NFH12	It is mandatory that the deliver an agreed backup plan, compatible with agreed SLA's, RTO and RPO.
[insert your answer here]	

6.7 Support and Monitoring

ID	DETAIL
NFS1	Helpdesk service is be provided to users of the product. This service is provided 24 x 7 via NZP Service Hub processes. NZP Service Hub operates 24x7, with teams based in Wellington and Auckland. Vendor support is communicated and managed via the NZP Service Hub.
[insert your answer here]	
NFS2	It is mandatory that the vendor provides support for the supplied products and services. The Respondent is to describe the options, including costing, for support: (i) Monday – Friday between the hours of 7am and 11pm NZ Time (ii) 24 hours a day, 7 days a week.
[insert your answer here]	
NFS3	It is desirable that support for the vendor supplied products and services must be responded to within 1 hour.
[insert your answer here]	
NFS4	Support tools or additional software required by the vendor or service agent to install, configure, support monitor the solution must be stated and approved as part of the overall solution design.

[insert your answer here]	
NFS5	It is mandatory that the Respondent provide proactive monitoring of the solution. Respondent is to describe how this could be provided.
[insert your answer here]	
NFS6	It is mandatory that the Respondent provide monthly reporting on (i) Availability (i) Capacity (ii) Security (iii) Performance Respondent is to describe an outline of the reporting to be provided.
[insert your answer here]	

6.8 Interfacing with adjacent systems

ID	DETAIL
NFI1	It is desirable that interfaces to NZP core systems via the NZP ESB, using web services.
[insert your answer here]	
NFI2	It is mandatory that the solution interfaces with NZP core systems to request & respond, send to or receive from core NZP systems, image and/or metadata. This may include but are not limited to: (iii) Merge of person details (iv) Issue or update of Firearms Licence details (v) Transfer of charge between persons (vi) Retrieve Person details (prisoner or firearms licence) (vii) Retrieve most recent Person details (viii) Retrieve charge group status (ix) Update from NZP Operational Reference data (x) Returning reference keys for image load and updates (xi) Retrieval of single thumbnail photo (person or photo reference) (xii) Retrieval of single full size photo (person or photo reference) (xiii) Retrieve all thumb-nails for a person/category(s) (xiv) Send removal of association between image and person (xv) Submit formal photo.
[insert your answer here]	
NFI3	It is mandatory that images provided to NZP core systems in: (i) JPG format and (ii) Associated meta data/reference keys (iii) Available as full image or thumbnail.
[insert your answer here]	

NFI4	It is desirable that the solution can import/load, NZP existing ABIS / Livescan facial images and metadata via a NIST file.
[insert your answer here]	
NFI5	It is desirable that the solution can import/load, NZP existing ABIS / Livescan SMT images and metadata via a NIST file.
[insert your answer here]	
NFI6	It is mandatory that the system(s) must interface to NZP Active Directory.
[insert your answer here]	
NFI7	It is mandatory that the system(s) must interface to NZP Exchange to send emails, both internally and externally to NZP.
[insert your answer here]	
NFI8	It is mandatory that the system(s) import a file of Firearms Licences from NIA for card production.
[insert your answer here]	
NFI9	It is mandatory that the system(s) export to file share the images and metadata for the Firearms Licence card producer.
[insert your answer here]	

6.9 Release & Deployment Management

ID	DETAIL
NFD1	It is mandatory that Software upgrades must be managed within an agreed release process.
[insert your answer here]	
NFD2	It is desirable that Enhancement requests can be submitted, applied and released within an agreed process
[insert your answer here]	
NFD3	It is mandatory that releases are acceptance tested by NZP prior to deployment into production.
[insert your answer here]	
NFD4	It is mandatory that deployment of the solution components to Acceptance Test / Pre-Production must be managed via NZP change management process.
[insert your answer here]	
NFD5	It is mandatory that deployment of the solution components to production must be managed via NZP change management process.
[insert your answer here]	
NFD6	It is mandatory that software deployed to NZP enterprise desktops (into production) must be packed by the managed desktop provider
[insert your answer here]	

6.10 Migration of existing data

ID	DETAIL
NFM1	It is mandatory that Image (JPEG) and associated metadata, including IMS photo reference number, be migrated from the existing photo management solution into the new solution.
[insert your answer here]	
NFM1	It is desirable that Images be migrated from ABIS/Livescan NIST files and submitted into a capture process within the new solution.
[insert your answer here]	

6.11 Reference Data

NZP core operational reference tables define attributes and associated values for information that is shared across multiple systems. Examples include: Hair Colour, Types of Clothing, Offence Codes, Court Outcomes, classification of SMT. These values are expected to change overtime, a start/end date is applied to each version of the attribute values.

Image & SMT management only, are attributes and associated value lists that are not shared outside the boundary of the proposed solution.

ID	DETAIL
NFB1	It is desirable that reference data that is shared or exchanged with NZP core operational systems will be sourced & maintained from the NZP core operational reference tables.
[insert your answer here]	
NFB2	It is desirable that individual entries within reference data tables will support multiple version based on an effective date. The date used within effective date validation will vary depending on the business process/form.
[insert your answer here]	
NFB3	It is allowable for reference data that is used for Image & SMT management only, may be managed by NZP Support Users directly within the solution.
[insert your answer here]	

6.12 Authentication & Authorisation

Authentication and authorisation of the users provide the ability to logon to the provided solution and gain rights to execute specific functions within the solution.

Terms:

- Authentication is the verification of a UserID & password to access the system.
- Authorisation is application of role based access control for an authenticated user.

ID	DETAIL
NFA1	It is mandatory that Users will be authenticated via NZP Active Directory, using NZP Enterprise userID & Password.
[insert your answer here]	

NFA2	It is desirable Authentication process will display the Code of Conduct - Acceptable Computer Use policy statement.
[insert your answer here]	
NFA3	It is mandatory that Users must be authorised to perform task/functions within the application that are associated with their role.
[insert your answer here]	
NFA4	It is desirable that User's application access *roles) will be controlled via NZP Active Directory.
[insert your answer here]	
NFA5	It is desirable that features will support single sign-on, users will be authenticated without re-entry of NZP Enterprise userID & Password.
[insert your answer here]	
NFA6	NZP application interfaces are trusted, specific users credentials are not required to initiate an interface transaction.
[insert your answer here]	

6.13 Security

ID	DETAIL
NFC1	Data Classification for the solution is "Restricted".
[insert your answer here]	
NFC2	It is mandatory that the transmission of user authentication details, such as user ID and password, over any network connect, must be secure and encrypted.
[insert your answer here]	
NFC3	It is mandatory that the authentication keys, such as passwords and encryption keys, when storied, are stored securely and never stored in clear text.
[insert your answer here]	
NFC4	The Respondent shall describe the access control mechanisms required/supported by each component'/function of the solution. Examples might be use of username/password or certificates.
[insert your answer here]	
NFC5	The Respondent shall describe the audit logging facilities included in the solution. This should include the points at which events are logged, what is recorded, where it is reported, what formats are used, how it is secured, and how this information is presented to auditors of the system.
[insert your answer here]	
NFC6	The Respondent shall describe how the solution ensures consistency and accuracy of system clocks across the various components that comprise the solution. Consistent and accurate system clocks ensure the integrity of audit trail and evidential trail.
[insert your answer here]	

NFC7	The Respondent shall describe any end point protection (including antivirus, anti-spyware, anti-malware, device port locking, and firewall), if any, is provided/supported by the solution.
[insert your answer here]	
NFC8	The Respondent shall describe what internet access, if any, is required for the solution.
[insert your answer here]	
NFC9	The Respondent shall describe how fixes and security patches are deployed and applied within the solution, including frequency.
[insert your answer here]	
NFC10	It is mandatory that the solution complies with the Certification and Accreditation requirements. This applies to both production and non-production environments.
[insert your answer here]	
NFC11	It is mandatory that all people accessing the system, including vendor project and support users, will be require a successful NZP Vetting prior to access being granted.
[insert your answer here]	
NFC12	It is mandatory that all people accessing the system, including vendor project and support users access the system via an individually issued NZP QID/password.
[insert your answer here]	
NFC13	It is mandatory that all people accessing the system, including vendor project and support users, comply with NZP rules and policies.
[insert your answer here]	
NFC14	It is desirable that the data is encrypted at rest.
[insert your answer here]	
NFC15	It is mandatory that the solution operates successfully in a firewalled network environment.
[insert your answer here]	

6.14 System Auditing

ID	DETAIL
NFG1	It is mandatory that activity (system and user) will be logged within the system. The Respondent is to describe who they record activity and transactions (User or system) within the solution.
[insert your answer here]	
NFG2	It is mandatory that the system Audit Logs will be available to NZP Assurance Group. The Respondent is to outline how the audit logs can be access and viewed by the NZP Security Team. Identifying any software required to enable this.
[insert your answer here]	

NFG3	It is desirable that the system integrate with current NZP SIEM solutions.
[insert your answer here]	

6.15 Testing & Training environments

ID	DETAIL
NFTE1	It is mandatory NZP Testing will be undertaken in a non-production environment. This includes interfacing to NZP test environments.
[insert your answer here]	
NFTE2	It is mandatory that Acceptance / pre-production deployment testing will be undertake in a non-production environment prior to deploying the solution or subsequent release into the production environment.
[insert your answer here]	
NFTE3	It is desirable that the Acceptance / pre-production environment be: (i) Production-like in configuration and resourcing (ii) Stable and subject to change management (iii) Integrated with (interface to) NZP core application testing environments. Eg NIA and Data warehouse, ABIS. (iv) Support 20 concurrent users.
[insert your answer here]	
NFTE4	It is desirable that System Test environment be available for functional fix-re-test and integration testing to Police system test environments. This is more volatile and with less rigid change control than the Acceptance / pre-production environment.
[insert your answer here]	
NFTE5	It is desirable that a Performance Testing be undertaken by the Respondent, and a report provided to NZP that demonstrates how the solution meets the performance requirements.
[insert your answer here]	
NFTE6	Defects will be managed via an agreed process.
[insert your answer here]	
NFTE7	It is mandatory that NZP will test releases of the product.
[insert your answer here]	
NFTE8	It is desirable that training will be undertaken in a non-production Training environment.
[insert your answer here]	
NFTE9	It is desirable that the Training environment will interface with NZP operational application training environments.
[insert your answer here]	
NFTE10	It is desirable that Training environment will be maintained and aligned with the production release/upgrade cycle, to support the ongoing training needs for the new staff and new application releases.
[insert your answer here]	

NFTE11	The Respondent shall outline how they support the non-production test and/or training environments both prior to the initial solution deployment and during the ongoing live of the solution: (i) Scheduled maintenance (ii) Availability and support (iii) Refreshing of data and synchronised with other systems
[insert your answer here]	

6.16 Testing

ID	DETAIL
NFTT1	It is mandatory that the Respondent complete a Factory Acceptance Test of the solution prior to handing to Police for Acceptance Test.
[insert your answer here]	
NFTT2	It is mandatory that the Respondent provide a report on the Factory Acceptance Test. This should include: (i) Test coverage (ii) Defects or issues not resolved.
[insert your answer here]	
NFTT3	It is mandatory that the Respondent provide evidence that the performance requirements are met by the solution.
[insert your answer here]	

6.17 Capabilities & Knowledge of Audience

ID	DETAIL
NFK1	It is desirable that Case Investigation features can be used without any specific training in the application.
[insert your answer here]	
NFK2	It is desirable Case Investigation training manual/user guide must be available to all users.
[insert your answer here]	
NFK3	It is mandatory that Image Management features are supported by a comprehensive training package. Initial training will be conducted on a single site.
[insert your answer here]	
NFK4	It is mandatory SMT Recognition features are supported by a comprehensive training package. Initial training will be conducted on a single site.
[insert your answer here]	

6.18 User Training

ID	DETAIL
NFUT1	It is mandatory that the Respondent provide the training for the following levels of users: (i) Help Desk Trainers - 2 ** (ii) Applications Support Group – 5 ** (iii) Productions Support Group - 5** (iv) Application Development Group - 3** (v) National work groups up to 15 users ** (vi) District Mentors (Train the trainer) up to 20 ** **Total number of trainees and roles to be trained to be confirmed. National work groups group includes National Biometrics Information team, Firearms Licensing and Missing Persons teams.
[insert your answer here]	
NFUT2	It is mandatory that NZ Police users will have access to self-paced learning material to ensure future training can be provided within Districts as and when required.
[insert your answer here]	
NFUT3	It is mandatory that the Respondent Training Deliverables include the following: (i) Skill and knowledge transfer (ii) System Administrations support skill transfer to appropriate agreed level (iii) Provide initial helpdesk knowledge base procedures.
[insert your answer here]	
NFUT4	It is mandatory that the Respondent provide the following Training Package: (i) Course overview, objectives and duration of the operational training that will be provided (ii) The expected training period for a general and a specialist user to become competent (iii) Hard and soft copy training documentation (iv) Scenarios and Hands-on exercises; required for District Mentors and administration personnel who will be operating the Image management system and peripheral equipment (v) Customised User Manual(s) (vi) Quick Reference Guide/s - including an overview of the key functions (vii) Modular presentation/demonstration (DVD) (viii) Online help (ix) FAQs (x) System Administration / Operations manuals (xi) Presentation and Demonstration.
[insert your answer here]	
NFUT5	It is mandatory that the Respondent Training delivered cover the following functionality: (i) formal photo line-up creation (ii) watch lists

	(iii) search facilities (iv) viewing images (v) biometric facial matching through facial recognition, and SMT matching (such as matching a suspect photo against a prisoner photo or a Facial composite photo against the known individual databases). (vi) reporting and presentation.
[insert your answer here]	
NFUT6	All appropriate documentation is available to be utilised on the NZ Police Standard Operating Environment. This includes, but is not limited to, being able to publish training and user documentation on the NZ Police Intranet and training support tools.
[insert your answer here]	
NFUT7	It is mandatory the Respondent supplied training of users is to be: (i) Provided in clear, comprehensible English (ii) Provided in a timely manner (iii) Comprehensive and complete, with appropriate level of detail (iv) User-friendly and effective in structure, format, duration and presentation.
[insert your answer here]	
NFUT8	It is desirable that the Respondent supply a softcopy of the training material without copyright so that it can be tailored to NZP training needs.
[insert your answer here]	

6.19 Project Management

ID	DETAIL
NFPM 1	The Respondent shall describe any Project Management, Software Development and System Support recognised standards they are audited and certified for (e.g. ISO/IEC, PRINCE2, CMMI, ITIL).
[insert your answer here]	
NFPM 2	The Respondent shall describe their standard Project Management approach, including the references and/or outlines of any frameworks and methodologies used.
[insert your answer here]	
NFPM 3	The Respondent shall summarise the qualifications and experience of their personnel in similar projects/deployments.
[insert your answer here]	
NFPM 4	The Respondent shall list describe their intended roles and involvement in this project.
[insert your answer here]	
NFPM 5	The Respondent shall describe how they intend to modify and customise their total solution to meet the requirements of this RFP.

[insert your answer here]	
NFPM 6	The Respondent shall outline the timeline required to implement the solution, including customisation and testing.
[insert your answer here]	
NFPM 9	The Respondent shall describe their intended approach towards long term proactive support and monitoring of the implemented solution, including but not limited to: (i) Support capabilities (Helpdesk) (ii) Location of their support services (iii) Capabilities for remote access and assistance (iv) Availability of support services (e.g. 24/7, work, hours, weekends etc.).
[insert your answer here]	
NFPM 10	The Respondent shall outline the approach the project **will** use to ensure quality control of the (i) Solution (ii) Project execution.
[insert your answer here]	

6.20 Police Deliverables

ID	DETAIL
NFPD1	The Respondent is to provide a details list of all requisite solution component specifications that are to be provided by Police in order for the System to operate in accordance with their proposal. The list should include but is not limited to hardware, software, cabling, interfaces, configurations, services, permissions, licenses and equipment.
[insert your answer here]	
NFPD2	The Respondent is to detail all assumptions that have been made in regard to any existing aspects of the Police ICT environment that are required in order for the system to operate in accordance with their proposal.
[insert your answer here]	

7 Future Strategic

The following may be required to support the future strategic of New Zealand Police. Describe how your solution will support each of the following requirements:

ID	DETAIL
FTR1	Facial Recognition capability to include using photos 'searched' from ABIS2 by an 'API' request via the Police ESB. Likely examples are ABIS2 connectivity to other Government agencies biometrics solutions for passport photos, drivers licence photos, etc.
[insert your answer here]	
FTR2	Ability for ABIS2 solution to automatically generate key image meta-data information, supplementing the meta-data manually captured. Likely example is 'red spider on neck' can be captured and is searchable. This may be occur during initial loading, but over time when more image patterns are quantified, these can be collected automatically against stored images.
[insert your answer here]	
FTR3	Ability to import CCTV feed into IMS, identify and image or images for recognition searching.
[insert your answer here]	
FTR4	Deliver functionality on an IOS mobility device.
[insert your answer here]	

END DOCUMENT

TN/18/03 A

This Pricing Template is provided as a guide and format for the pre
ensure that all detail requested in Sec

Respondents name:		
Service	**Unit Price excluding GST**	**Unit**
Licencing Costs		
Image Management Solution		
Facial Recognition		
Scars Marks Tatoos /Clothing		

Provide any price breaks on quantity (min/max)

Provide information on assumptions made

Service	**Unit Price excluding GST**	**Unit**
Development and Deployment		
Development (tendered price)		
Deployment (tendered price)		
Project Management (tendered price)		

Provide Information on assumptions made

Hourly Rates for each discipline		
e.g Developer/ Project Manager		
insert lines as necessary		

Service	**Unit Price excluding GST**	**Unit**
Training and Support		
Annual Support and Maintenance		
Initial Training - (tendered price)		

Provide information on assumptions made

Hourly / Daily Rates for each discipline as applicable		
e.g Additional training days		
insert lines as necessary		

ABIS 2

sentation of price, it is incumbant on the Respondent to
tion 4 of the RFP is provided.

Comments

Comments

Comments