IMS Photo Manager and the ABIS 2 Project Privacy Impact Assessment

Prepared by the National Biometric Information Office (NBIO) & the Assurance Group, NZ Police

February 2022 (update)

Executive Summary

The ABIS 2 Project aims to upgrade image management with an enhancement to the existing IMS PhotoManager utilising DataWorks Plus's WebWorks Plus system; which deals with the loading and use of images taken from individuals and the upgrade of the IMS facial recognition capability using NEC's FACE Plus software. The package is being provided by DataWorks Plus. Further interface work between IMS PhotoManager and the NIA Police system is being developed in-house.

The improved system will also enable a comparison of scars, marks and tattoos. The new system is not creating a new collection of information, nor is it operating in a "public facing" capacity.

The addition of a more up to date facial comparison system will give Police the capability to load, search and compare crime scene / incident images from a variety of sources (including but not limited to static images captured from CCTV footage and digital photographs) with poorer quality facial images in the footage against known identity images. The electronic searchable tattoo image database will also increase Police's intelligence capability.

The capability to Livestream CCTV is not included in the Business Case, the RFP requirements, the detailed design or the build.

The IMS-Photo Manager image comparison tool will be operated and managed from the National Biometric Information Office (NBIO) and will only be available to trained staff within the NBIO and trained district staff grouped as IMS Investigators. The latter group is responsible for providing districts with photographic Line-up capabilities.

The system will be governed by defined business processes and system rules which will be created before deployment. There will be a reporting capability for user activity for auditing purposes.

A range of risks arise around the governance and management of the system; access to the tool by the wider policing capability; and, transparency with the public about Police's uses of the system. In Privacy Act terms the relevant Information Privacy Principles include IPP 3 (Advice about the use of collected personal information; IPP 5 (Security); IPP 8 (Accuracy of Personal Information); and IPP 10 (Use of personal information).

The recommendations within the report are –

Recommendation 1: Establish an administrative and user system within the NBIO that safeguards the system to the management and use of trained and experienced staff only and potential links will be provided for intelligence purposes only. The establishment of Active Directory Groups should only give authorised users the capability. Only NBIO, District IMS Investigators and ICT Administrators ought to have access. Comprehensive system rules and reporting tools will ensure User Activity is recorded and reportable for audit purposes.

Recommendation 2: Establish administrative oversight of the system so that results are overseen by NBIO staff and scrutinised by them prior to release to investigative staff. All potential match reports to be generated by trained NBIO staff members.

Recommendation 3: Ensure that the Active Directory is well managed to ensure that particularly District IMS Investigators have access permission removed when no longer required.

Recommendation 4: Create and manage an active audit process that acts as a deterrent to misuse of the IMS.

Recommendation 5: Establish a business process where requests for searches of the image database are submitted in writing, approved by a supervisor and tied to a function of Policing.

Recommendation 6: Establish oversight of IMS Photo Manager by an appropriate governance group that receives regular reports detailing the effectiveness of the system and provides assurance that the operation of the system remain ethical and lawful.

Recommendation 7: Establish a communications plan to signal widely the use of the IMS Photo Manager system within the ABIS 2 project.

Overall, the estimated risk rating without controls sits at *High 14 to High 22.* If effective controls and mitigations are deployed the residual risk rating is likely to be *Medium 6 to Medium 13.* The residual risk would be within Police's acceptable risk rating. Table 2 at the end of the report details the identified risks and suggested mitigations and controls.

Privacy Impact Assessment

Why a Privacy Impact Assessment?

A PIA examines a change, project or system to evaluate how, and to what extent, it might impact on individual privacy. It also identifies inherent risks pertinent to the Police operational use of a business process or tool. The PIA process is about designing privacy into the project, to ensure that risks are identified early and processes, products and safeguards are designed with privacy in mind from the outset. It's about setting the right course early.

This assessment has a focus on ABIS 2 project (Automated Biometric Identification Solution) which is an umbrella term that encapsulates a suite of products used within Police Biometrics, including the original AFIS (Automated Fingerprint Identification system). ABIS 2 specifically refers to an upgrade to the photo Management (IMS) aspects of Biometrics, including improved facial comparison software and the capture of Scars, Marks and Tattoos at the point of capturing other Biometric data

at police stations. The assessment is intended to assist the National Biometric Information Office (NBIO) to avoid privacy pitfalls and deploy ABIS in a way that strikes an appropriate balance between business benefits and good privacy practice.

Like all risk assessment reports, this PIA should be viewed as a living document, which ought to be revisited later in the process either to accommodate changes to the project or when the tool has merged into 'business as usual'. Over time it should be used to establish how risks have been managed and whether controls continue to be effective.

Scope of this PIA

This PIA looks at the privacy impacts of the deployment of a new and upgraded tool that will assist the NBIO to manage its growing image database. The new system is not creating a new collection of information, nor is it operating in a "public facing" capacity. The NBIO currently has the responsibility for managing Police's fingerprint records and images library. The images are drawn from a range of existing collection practices including custody photographs, firearms licence photographs, informal photographs of suspects collected in connection with law enforcement activities and missing persons. The PIA will cover the deployment of the technical tool and management of the images data base. Not necessary within the risk assessment is examination of collection (IPP 1 – 4) , (but the expectations of good management of personal information that derive from them are, concepts such as transparency around why and how we are using information),retention (IPP 9) or use of the images as these practices are current business as usual and will not change as a result of the ABIS 2 upgrade.

The assessment will consider the issues that arise in the deployment of the Image Management System (IMS Photo Manager). Risk will be identified and quantified by reference to Police's risk matrix.

This version of the original PIA dated October 2020 is updated to review the consequences of additional staff outside of the NBIO having access to the IMS.

Privacy Considerations

Several lenses are used to assess a project – Information Privacy Principles (IPPs) in the Privacy Act; Privacy by Design© [1]; and, principles used in the deployment of data analytics or emergent technologies. IPPs are outlined in the Privacy Act 2020 and provide for responsibilities around how agencies may collect, store, provide access to, use and disclose personal information. They encourage a view right across the lifecycle of the information from collection to disposal. They are designed to ensure that an agency can use personal information to achieve its lawful purposes efficiently and effectively, while protecting the privacy rights of the individuals the information is about. Although sourced from the Privacy Act, these IPPs are reflective of globally accepted best privacy practice, and provide an effective framework through which to assess privacy issues in the context of the IMS Photo Manager.

In addition, the seven principles of Privacy by Design© are relevant. These help to build privacy controls into systems, technologies and processes. If implemented correctly, individuals should not have to take any action to protect their privacy – the system's design achieves this by default.

Lastly, emergent technologies that use algorithm calculation for analytical purposes require further consideration of their use from a fairness and ethical perspective. The Privacy Commissioner's

[1] Privacy by Design© 7 Principles - Privacy measures should be proactive not reactive; Privacy should be the default setting; Privacy should be embedded into design; Aim for full functionality rather than viewing privacy in opposition to other interests; Ensure end-to-end information security; Promote visibility and transparency of risks and solutions; and, make sure systems are user-centric.

Principles for the Safe and Efficient Use of Data Analytics – May 2018[2] point to considerations that include ensuring that the tool delivers a clear public benefit; the data is fit for the purpose of analytics; privacy and ethical issues are explored; where appropriate the technological use is transparently used; maintain human oversight of the process including decision making; and, adequate governance.

Image Management System (IMS Photo Manager)

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 current 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. However, the system has very limited and outdated facial recognition capability. Currently scars, marks and tattoo details are held in a coded/textural format. Police have no image based capability to capture, classify, search and match scars, marks and tattoos and logos for intelligence or identification purposes.

The addition of a more up to date facial comparison system, via IMS-Photo-Manager~~,~~ will give Police the capability to load, search and compare crime scene / incident images from a variety of sources (including but not limited to static images captured from CCTV footage and digital photographs) with poorer quality facial images in the footage against known identity images. The electronic searchable tattoo image database will also increase Police's intelligence capability.

The capability to Livestream CCTV is not included in the Business Case, the RFP requirements, the detailed design or the build.

Purpose of the change, including any projected benefits to your organisation or to the individuals affected.

IMS Photo Manager will provide a more advanced electronic facial comparison system that improves image quality and can provide more opportunities for matching, particularly with poorer quality facial images often encountered with CCTV footage. This improved searching and matching capability will reduce investigation time and prevent crime and victimisation rates. It will provide a significantly higher level of success at identifying suspects/offenders when compared with manual searching, leading to early perpetrator intervention and reducing the time taken to make the links.

Current technology and processes do not allow NZ Police to capture and utilise individuals' identifying particulars, scars, marks and tattoos (SMT) in a timely manner. This leads to the opportunity for re-offending and re-victimisation. The investigation time involved in comparing images will be significantly reduced, meaning greater time for other investigative activity.

Both facial and SMT images from offenders will be captured within stations/sites and retained under ss.32 and 33 of the Policing Act 2008.

The IMS Photo Manager enhancement will enable records to be stored and classified in categories and sub-categories, and in addition to facial comparison capability, searches can be made on soft biometrics such as scars, marks and tattoos.

---

[2] https://www.privacy.org.nz/publications/guidance-resources/principles-for-the-safe-and-effective-use-of-data-and-analytics-guidance/

The IMS Photo Manager image comparison tool will only be available to trained staff within the NBIO who will be trained to use the system, governed by defined business processes and system rules. These rules and protocols will be established before the IMS is deployed. There will be a reporting capability for user activity for auditing purposes.

A further user group has now been added to enable Districts to have a photograph Line-up capability available for investigations. This group is known as IMS Investigators and numbers approximately 70 persons. Like the NBIO staff this group will also receive appropriate training on how to use the IMS. They will also be subject to the rules and protocols.

The Nature of the Information.
Facial images in the Police images collection include Formal Offender (custody suite photographs), Child Sex Offender images, Returning Offender images, missing person's images, and Firearms Licencing photographs. Images of scars, marks and tattoos are also collected from the custody suite and from registered Child Sex Offenders. (See Appendix 1 for details of the collection processes). The formally acquired images are used to compare images on a variety of mediums that are provided to Police by witnesses to crime or acquired by Police through criminal investigative processes.

Current and projected volumes of images are contained within the table below, showing that at any stage the Photo Manager system will have in excess of 2 million images to manage.

Category	**Historic Records** (Current as @ business case 2016)	**Estimated Additional Records per Annum** (Future)
Image Management - Prisoner	1.85M from 800,000 individuals	50,000 per annum
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
Image Management - Missing Persons	200	300 per annum
Image Management – Child Protection (Child Sex Offender Register)	1,500	2,300 per annum
Facial Recognition Search, Compare, Match and Report	Nil	At least 15,000 per annum
Photo line-up Production	12,000 (Time to prepare standard line-ups: 20 – 60 minutes)	15,000 (Time to prepare standard line-ups: 10 minutes)
Scars Marks and Tattoos and Logos Capture, Search, Match and Report	2,500	30,000 (estimated)

Table 1 - Current and Projected Data within the Photo Manager System

Initial risk assessment

The images library contained with IMS Photo Manager comprise a significant volume of images. These images will be used for comparison with photographs that Police wish to identify for a variety of law enforcement reasons. The tool used for comparison purposes uses algorithms deployed to match a defined quantity of features to produce a potential match or matches.

The risks in deploying the facial recognition aspect of the technology arise out of appropriate deployment, use and security (IPP 10 – Appropriate use; IPP 5 – Security and IPP 8 – Accuracy) of the comparison tool and the image library, ensuring that the tool is only used for a lawful business purposes (IPP 1 – Purpose) and ongoing oversight of the deployment. There are potential 'transparency' issues that require managing (IPP 3 – Advice about the use of collected information). The remaining IPPs are not relevant to this deployment of IMS Photo Manager and the use of existing and to be collected personal information.

Use and Deployment of the Facial Comparison Tool

The proposed application uses industry-leading algorithms and can be tasked to perform facial comparison searches for both newly-acquired images, as well as previously-enrolled images. Newly-acquired image queries can be configured for automatic searching and on an ad-hoc basis as new records are generated. Previously-enrolled image queries can also be performed on an ad-hoc basis by authorized users.

The biometric matching process is controlled by the user so that only the best few images are returned as matches in descending order from the highest match score. The Administration Module allows Administrators of the system to set the facial match scoring thresholds to determine what query scores are considered a match or non-match. Only images that are above the match score threshold will be displayed to the user.

There is a risk that if the system is not managed by trained and competent users, the tool may be used in an unnecessarily liberal manner therefore returning matches that are questionable. This raises a risk of contravening IPP 8 which requires personal information not to be used or disclosed without taking steps to ensure the information is accurate, up to date, complete, relevant and not misleading. This risk would be *likely* if the tool were to be used by untrained and inexperienced users. This may result in *moderate* to *major* consequences including scrutiny by public media, scrutiny from the IPCA or the Privacy Commissioner either on their own initiative or driven by complaints from individuals who have been incorrectly identified as persons of interest to the Police. The incorrect identification of individuals is a potential risk to the individuals that may result in unnecessary or arbitrary arrest or detention. Currently there is a high level of public concern about emergent technologies and any misuse or perception of misuse creates media and political interest, and potential harm to individuals. It is likely that unless adequate controls are put in place the inherent risk would sit at *High 17 to 22*.

Appropriate controls would include limiting the deployment of the algorithm to only those trained members of the NBIO. Training ought to include a high level understanding of the effect of any changes that the user can make to the way the tool carries out the search function. Administrative settings ought to be determined and applied consistently within the system. These setting ought to be a part of the business protocols and rules for using the system. In addition the images database and the results of searches, with the exception of the District IMS Investigators, ought to be managed solely by the NBIO group so that the integrity of the images within the database and the

use of the comparison tool are confined to highly trained users and consistent algorithmic thresholds are applied. Decisions about whether a matched image is appropriate for release to an investigation team should remain with the NBIO staff.

Recommendation 1: Establish an administrative and user system within the NBIO that safeguards the system to the management and use of trained and experienced staff only and potential links will be provided for intelligence purposes only. The establishment of Active Directory Groups should only give authorised users the capability. Only NBIO, District IMS Investigators and ICT Administrators ought to have access. Comprehensive system rules and reporting tools will ensure User Activity is recorded and reportable for audit purposes.

Recommendation 2: Establish administrative oversight of the system so that results are overseen by NBIO staff and scrutinised by them prior to release to investigative staff. All potential match reports to be generated by trained NBIO staff members.

Applying these controls will reduce the likelihood to *unlikely* with the consequences remaining at *moderate* to *major.* The residual risk is likely to move to Medium 9 to 13.

Security

The IMS has a range of information management controls that apply to authorized users who work within the system.

Active Directory

An Active Directory is used to grant individual or group access to the IMS System. Early intention was that the system would be managed and used solely by dedicated staff within the NBIO. This meant that granting and removing access was tightly managed with the NBIO. The inclusion of District IMS Investigators introduces a risk that District staff may not have access terminated appropriately when they change roles or leave Police. An employee who leaves Police has general access removed early through withdrawal of an enterprise email address. An employee who changes roles and remains in Police will need to be promptly removed from the active group to ensure that no further access is enabled. The risk is that a disaffected employee with access permission might be motivated to misuse the images within the system. As mentioned earlier technology that involves AI and, in this case, facial recognition are a source of wide public concern. There are a range of systems within Police that are vulnerable to aberrant employee behaviours but wisely used active directory would reduce the risk for the IMS. Without proper use of the active directory the inherent risk would be *Medium 8 to High 14.*

Recommendation 3: Ensure that the Active Directory is well managed to ensure that particularly District IMS Investigators have access permission removed when no longer required.

Prompt action to remove employees who no longer work within the IMS will assist in reducing risk to the data holdings and result in a residual risk from *Low 5 to Medium 9.*

Audit

Access to the IMS system also enables access to a substantial amount of image data. Misuses of this data is likely to cause a significant embarrassment to Police particularly in the context of the emergent technology component of the system. However, in a personal information context there is the likelihood of misuse causing significant harm to individuals.

IMS Investigators will have general access to the IMS. A feature of the system means that users who log onto the system are first confronted with the last 8 images that have been added to the system. Permitted users have access to the wider system so this display does not introduce undue risk. However, adequate audit capability will help reduce any inherent risk.

Together an active directory and comprehensive audit capability provide security options to prevent and detect aberrant behaviours by employees. Audit that includes proactive capability is also more desirable than relying on audit to detect passed behaviors. The latter introduces a heightened possibility that individuals who have an interaction with Police may suffer harm.

IMS has comprehensive audit report capability which includes

- 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

It is desirable that the audit capability is used proactively to reduce the potential harm that may arise from misuse of the IMS data. Ideally active audit should be designed to detect misuse of data before the misuse causes harm. At least regular random audits ought to be a feature of security oversight of the IMS. In the context of the limited numbers of staff that have access to the IMS platform random audits that are well managed and visible to relevant staff are likely to provide a suitable deterrence to misuse of the system. Without active and visible audit of staff use of the IMS the inherent risk would be *Medium 8 to High 14.*

Recommendation 4: Create and manage an active audit process that acts as a deterrent to misuse of the IMS.

Proactive and visible audit activity is likely to result in a residual risk from *Low 5 to Medium 9.*

Lawful Business Purposes

The IMS Photo Manager is deployed to assist with Police's functions of law enforcement and keeping the community safe. Operational business groups should only seek facial comparisons by trained NBIO staff for a range of appropriate business reasons from the comparison of suspect images with those in the image database to establish the identity of a suspect for a crime, through to locating better images of lost or missing persons or establishing identity of an unidentified deceased individual.

It is *possible* that the image library and the facial/image comparison tool could be misused or abused if careful oversight of requests for access to the system are not scrutinised. IPP 10 expects an agency to only use personal information for the purpose for which it was obtained. Personal information within the scope of the NBIO is acquired for law enforcement purposes or public safety. It is important to maintain oversight of the use of that information so that unlawful purposes are not applied. Like the previous risk category, abuse of the tool would expose Police to unwanted attention from a number of public quarters and have a *moderate* to *major* impact on the trust and confidence of Police. In addition misuse of the system may have a significant impact on individuals who are the subject of aberrant searches of the database. The inherent risk would be *High 17 to 22*.

Controlling access to the image library and the corollary use of the facial/image comparison tool ought to include a business process where requests for searches of the image database are submitted in writing seeking access to the system. All 'suspect' searches will be submitted via Lotus Notes (or a new alternative) with full details of the offence, including Case (DOCLOC) Reference, Submitting Officer and details of the Supervisor Authorising Submission. All 'suspect' images will be dealt with as Exhibits; entered into Police Register of Property (PROP) prior to submission. The Chain of Evidence / continuity will be maintained throughout the process. The requests ought to describe in sufficient detail the reason for the request and the particular Police function that is at the heart of the request. In addition the request ought to be approved by the requester's supervisor in all cases to demonstrate the legitimacy of the request and the business reason for it. Records of the requests and responses ought to be maintained indefinitely to contribute to audit and assurance reporting.

Recommendation 5: Establish a business process where requests for searches of the image database are submitted in writing, approved by a supervisor and tied to a function of Policing.

By establishing a business process that ensures oversight of the requests for access to the image database the likelihood of misuse of the system would be reduced to *rare* with the residual risk reduced to *medium 6 to 10.*

Ongoing Oversight of IMS Photo Manager

The community interest and tension around the deployment of emergent technologies such as facial recognition or facial and image comparison tools receives global attention at present, particularly where the tools are deployed in the law enforcement space. Recent public furore over the NZ Police's interest in the Clear View AI tools created heightened interest in our use of emergent technologies. Police's interest in Clear View AI is not a relevant interest in the ABIS 2 Project. The Commissioner of Police has set an approval and governance oversight for all projects that involve emergent technologies. NECs algorithm fits into the category of emergent technologies.

In addition to there being a requirement to run the deployment past executive and other governance arrangements to approve the deployment, it is very appropriate to ensure that the ongoing governance of the system is established. Governance is an aspect of meeting our general obligations within the relevant IPPs including security (IPP 5), accuracy of the tool (IPP 8), and appropriate use of the personal information provided to and used by the NBIO (IPP 10). The absence of ongoing business governance risks the tool not receiving sufficient oversight to ensure that controls remain fit for purpose, that the tool remains lawfully used and that the system continues to provide a benefit to Policing and contributes to keeping the public safe. Without

ongoing governance oversight it is *possible* that the system may fail to deliver a safe and defensible service or its use is inadvertently widened beyond the current stated purpose, known as function creep. Were the system to become subject to external scrutiny Police would be seriously criticised for not establishing governance over the system. This would be unacceptable, particularly in the context of an emergent technology, as Police might be seen as potentially cavalier about its oversight of technology, an unacceptable rhetoric for a law enforcement agency. The consequences of an unexpected event may be *moderate* to *major* depending on the context, with an inherent risk rating of *High 14 to 18*.

Establishing governance oversight to an appropriate new governance group ought to involve regular reporting to that group in a '3 lines of defence' assurance mode. That would at least mean reporting that demonstrated the worth of the tool by reference to the number of requests; the success of the system with examples; the time saved if capable of quantification; and, updates about the reliability and effectiveness of tools capability in identifying images correctly. Additionally, periodic reporting ought to demonstrate that the controls remain in place, remain effective and if not recommendations for any changes are made, if warranted. Demonstrating that the efficacy of comparisons continues to be overseen by human decision making is an important aspect of ensuring that the system remains lawful and ethical. The NBIO intends to supply prescribed and ad hoc reports as required.

Recommendation 6: Establish oversight of IMS Photo Manager by an appropriate governance group that receives regular reports detailing the effectiveness of the system and provides assurance that the operation of the system remain ethical and lawful.

Regular and constant assurance reporting to an appropriate governance group will ensure that the integrity of the system is maintained, that it continues to provide a benefit to the business and provide assurance that the tool is used ethically and lawfully. The likelihood of an unexpected event would reduce to *unlikely* or *rare* and the consequences while remaining *moderate* to *major* the residual risk value would reduce to Medium 6 to 13.

Transparency

As mentioned earlier in the report there is a heightened community interest in emergent technologies such as facial recognition and artificial intelligence. That interest is particularly heightened where the technology is deployed overseas and more so when the state agency is a law enforcement agency. Media coverage has focussed on the deployment of technology in public places, for example at large sporting events where facial recognition tools are used to locate wanted persons or persons of interest. IPP 3 expects that an agency will communicate with individuals at the time of collection of their information and while this is not relevant in the context of IMS Photo Manager, the wider expectation of transparency around use of information remain good business practice

New Zealand Police will not be using IMS Photo Manager technology in a public facing way. The correct rhetoric is that Police is deploying the tool to assist with searches of its existing and growing images library. Images that Police lawfully acquire as a consequence of carrying out its functions under the Policing Act. As a result it is important for Police to be open and transparent about our deployment of IMS Photo Manager to dispel any potential unrealistic views of the project and the system.

The inherent risk of not getting on the front foot and being transparent about the project is that public thought will be influenced by incorrect assumptions about the extent of the use of the system, therefore bringing Police into unnecessary negative commentary about its use of technology.

Recommendation 7: Establish a communications plan to signal widely the use of the IMS Photo Manager system within the ABIS 2 project.

The risks to Police through introducing the IMS Photo Manager technology will be reduced if a communications plan includes –

- Consultation with the Privacy Commissioner's office before full deployment
- At appropriate times, media statements about the deployment of IMS Photo Manager accompanied by assurances about the controls and limits of the system
- Commentary of the Police Website under the area 'How We Manage Personal Information' detailing how we deploy IMS Photo Manager

Table 2 - Inherent Risk – Residual Risk & Recommended Controls

Inherent Risks	Recommended remedies and controls and Residual Risk	Privacy Act Principle applicable	Date Considered or Implemented
Risk 1 & 2 - There is a risk that if the system is not managed by trained and competent users, the tool may be used in an unnecessarily liberal manner therefore returning matches that are questionable. It is likely that unless adequate controls are put in place the inherent risk would sit at *High 17 to 22*.	Appropriate controls would include limiting the deployment of the comparison tool to only those trained members of the NBIO. Training ought to include a high level understanding of the effect of any changes that the user can make to the way the tool carries out the search function. In addition the images database and the results of searches, ought to be managed solely by the NBIO group so that the integrity of the images within the database and the use of the comparison tool are confined to highly trained users. Decisions about whether a matched image is appropriate for release to an	IPP 8 Accuracy of personal information	

	investigation team should remain with the NBIO staff. Applying these controls will reduce the likelihood to *unlikely* with the consequences remaining at *moderate* to *major.* The residual risk is likely to move to Medium 9 to 13.		
Risk 3 & 4 There are risks inherent in not managing who has access to the IMS and not monitoring or auditing staff use of the information within the IMS. It is possible that data within IMS is misused causing reputational harm to Police and potentially harm to citizens whose information is in IMS. The inherent risk sits at *Medium 8 to High 14*	Necessary controls include ○ an Active Directory process that ensures that only appropriate staff are given access to IMS and that their access is efficiently withdrawn when they leave the workplace ○ regular proactive audit if users activity within the IMS Applying these controls will likely result in a residual risk of *low (unlikely and minor) to medium 9 (unlikely to moderate)*	IPP 5 Security IPP 10 & 11 Appropriate Use and disclosure	
Risk 3 - It is *possible* that the image library and the facial/image comparison tool could be misused or abused if careful oversight of requests for access to the system are not scrutinised. The inherent risk would be *High 17 to 22*.	Controlling access to the image library and the corollary use of the facial/image comparison tool ought to include a business process where requests for searches of the image database are submitted in writing seeking access to the system. The requests ought to describe in sufficient detail the reason for the request and the particular Police function that is at the heart of the request. In addition the request ought to be approved by the requester's supervisor in all cases to demonstrate the legitimacy of the request and the business reason for it. By establishing a business process that ensures oversight of the requests for access to the image	IPP 10 – Appropriate use of personal information	

	database the likelihood of misuse of the system would be reduced to *rare* with the residual risk reduced to *medium 6 to 10.*		
Risk 4 – It is appropriate to ensure that the ongoing governance of the system is established. The absence of ongoing business governance risks the tool not receiving sufficient oversight to ensure that controls remain fit for purpose, that the tool remains lawfully used and that the system continues to provide a benefit to Policing. The consequences of an unexpected event may be *moderate* to *major* depending on the context, with an inherent risk rating of *High 14 to 18*.	Establish oversight of the IMS Photo Manager system by appropriate governance group that receives regular reports detailing the effectiveness of the system and provides assurance that the operation of the system remain ethical and lawful. Regular and constant assurance reporting to an appropriate governance group will ensure that the integrity of the system is maintained, that it continues to provide a benefit to the business and provide assurance that the tool is used ethically and lawfully. The likelihood of an unexpected event would reduce to *unlikely* or *rare* and the consequences while remaining *moderate* to *major* the residual risk value would reduce to Medium 6 to 13.	IPP 5 Security; IPP 8; and IPP 10.	
Risk 5 – There is an inherent risk of not getting on the front foot and being transparent about the project resulting in the public thought being influence by incorrect assumptions about the extent of the use of the system, therefore bringing Police into unnecessary negative commentary about its use of technology.	Establish a communications plan to signal widely the use of the IMS Photo Manager system within the ABIS 2 project that includes – ○ Consultation with the Privacy Commissioner's office before full deployment ○ At appropriate times, media statement about the deployment of IMS Photo Manager, accompanied by assurances about the controls and limits of the system	IPP 3 – advising individuals about how their information is used	

	○ Commentary of the Police Website under the area 'How We Manage Personal Information' detailing how we deploy the IMS Photo Manager system.		

Appendix 1

Category Overview - Legislation / Authorisation

The images held by Police are stored in logical categories; Formal (which includes Offender, , Customs, Child Sex Offender, and Returning Offenders), Firearms Licence holders, Missing Persons and Suspect images. The following table sets out the overview for each category.

Category	Legislation / Authorisation / Policy	Comments
Offender	Policing Act 2008 ss.32, 33, 34 34A	Identifying Particulars Taken on Arrest or Summons. Retained on Conviction
Customs	Memorandum of Understanding (2015) between NZ Police and NZ Customs; Schedule 4: Arrest and Prosecution / Arrest and Prisoner Processing Also letter of clarification (20 November 2015) from Commissioner Mike Bush to NZ Customs	Police agree to receive into custody, process and hold, persons arrested by Customs officers on behalf of Customs. Normal processing procedures must be completed by Police. As soon as practicable following the filing of charges, Customs will provide the Police National Biometric Information Office with charging information, for the purposes of ensuring the biometric records are linked to relevant charge information. The information will be sent electronically to the National Biometric Information Office and will include: • Arrested person's name, sex and date of birth; • Date of arrest; • Police station where the person was processed; • Justice Person Record Number (PRN); • Details of the charges and appropriate charge codes. • The National Biometric Information Office will ensure the charging • information for the arrested person will be linked to their electronic biometric records; in NIA the biometrics are held in relation to charges on the associated Justice PRN.

Child Sex Offenders	Child Protection (Child Sex offender Government Agency Registration) Act 2016	s. 32 Identifying particulars and other information may be stored by Police
Returning Offenders	Returning Offenders – Returning Offenders (Management and Information) Act 2015	s. 8 Purpose of obtaining information for use by Police for any lawful purpose s. 9 Police may request returning offender to provide identifying particulars s. 10 Police may detain returning offender for purpose of taking identifying particulars s. 11 Police may take identifying particulars s. 12 Storage, etc, on Police information recording system of identifying particulars
Firearms Licence	Arms Act 1983	Firearms Licensing Application form: *'The information you provide on this form is collected for the purpose of administration of the Arms Act 1983. NZ Police will hold, store, use or disclose the personal information collected in accordance with the provisions of the Privacy Act 1993. This means that, where necessary, NZ Police may use or disclose your personal information to enable it to carry out its lawful functions, including prevention, detection, investigation and prosecution of offences. Please refer to the Privacy section of our website for more information'.* Use of the Firearms Licensing Application form photograph is essential for initial vetting and for continued integrity of the licensing process and management of firearms licences.
Missing Persons	Police instructions – Missing Persons Common Law POL 65 Publicity Form	Photographs of Missing Persons are obtained to assist with enquiries to locate or ensure the safety of that person. These enquiries are carried out under the common law power to make all necessary enquiries to protect and preserve life. Part of the enquiry involves obtaining from the informant a recent photograph of the missing person and a signed authorisation for Publicity form POL 65. Not all Missing Persons photographs will be loaded to the Missing Person database. This process will be managed by the Missing Person Unit.
Suspect		Suspect images will be held on the unsolved suspect database and are images of unknown person image from a scene / incident. They will be treated as an exhibit being entered on PROP system and linked to a NIA Case with a NIA Forensic Examination. The submitting officer will select a forensic test for the exhibit. The Test being Facial Comparison. This is the same process as when officers submit Fingerprints or DNA for examination; they select a Test. Submission for a Facial Comparison examination will need to be authorised by a supervisor, as with other forensic exhibits with subsequent tests / analysis. This Facial Comparison capability may be used as an

		alternative/additional option for 'identity sought' when districts publish photos of individuals on Police Intranet / websites etc. It can also be used for the linking of scenes / incidents where the same individual is involved. The images will be used for intelligence / investigation purposes. These images will be used for facial comparison purposes and searched against the known person databases (Offender, Voluntary, Customs, Child Sex Offenders, Returning Offenders, Firearms Licence holders and Missing Persons) to provide intelligence / identity of the individual featured in the Suspect image. The system cannot be used for Facial Recognition of Live streaming or within a public facing context.