AVSEC Queue Counting & Wait Time Proof of Concept Project:

Privacy Impact Assessment of Proposed Trial of Project

[Final: 25 May 2021]

Privacy Impact Assessment – Contents

Document version control	**Date**
First draft	12 March 2020
Second draft	05 June 2020
Third draft	17 July 2020
Fourth draft	03 August 2020
Fifth draft	05 August 2020
Sixth draft	14 August 2020
Seventh draft	21 August 2020
Final	25 May 2021

1. Project Summary

The Queue Counting & Wait Time Proof of Concept Project (**the Project**) by the New Zealand Aviation Security Service (**AVSEC**) proposes to use recognition based technology to count the number of people passing through a security screening area at an airport and produce a real time wait time for passengers waiting to be screened.

The Project will use the existing photos provided by airport identity card (**AIC**) holders to distinguish non-passengers from passengers and thus produce a count of the number of passengers and non-passengers using the security screening service.

The Project will initially be implemented as a trial at Wellington Airport (**the Trial**). The Trial will operate for 8 weeks. The Trial will be rolled out nationally if the Trial is determined to be successful.

The Project will face based biometrics technology to count passengers and non-passengers entering and exiting a security screening area, and this involves the collection of personal information – face based biometrics referred to hereon as an image . The purpose of this privacy impact assessment (**PIA**) is to assess the privacy implications of the collection of this personal information for the Trial and, to the extent that the details for the Project are known, to include those details of the Project in the privacy assessment.

The purpose of the Project

The Project will use facial recognition-based technology to count the number of people passing through a security screening area at an airport.

The technology will –

- produce a real time wait time for passengers waiting to be screened at a security area
- produce an accurate count of the numbers of passengers passing through a security area (by distinguishing non-passengers from passengers)

Any privacy risks or issues identified by the PIA will be considered and taken into account for the Trial, and also applied when the Project is rolled out at other airports around New Zealand.

The Project will enable AVSEC to accurately report on the services provided to passengers and non-passengers (as only the former pay the Aviation Security Service levy which funds AVSEC's activities). Other benefits will include better management of queues and wait times, better resource management of rostering for security check points, and by providing a visible wait time, provide a more efficient security screening service to passengers and non-passengers.

2. Scope of the PIA

2.1 Scope

The Trial and Project will be managed by the AVSEC Head Office Innovation Team, supported by the Workforce and Business Improvement Team, and the Information Technology Team.

The technical support and hardware, including the cameras for the Trial, will be provided by the Service provider, The recognition analytics are manufactured by the Recognition Platform software. The data generated by the Trial will be stored on the Cloud server that is located in New Zealand and dedicated for the use of New Zealand government agencies.

At this stage, the proposed IT configuration for the national roll-out of the Project will be revisited at the conclusion of the proof of concept trial and is yet to be confirmed.

This PIA considers the privacy implications of the collection of matching datasets from passengers and non-passengers passing through the security screening area for the Trial, which will be located at Wellington airport. The PIA assesses the collection of these matching datasets, which are personal information, against each of the 13 information privacy principles contained in the Privacy Act 2020.

2.2 The process

This PIA has been prepared by an independent barrister and solicitor, , .

was briefed on the Project by the AVSEC Strategic Development Group's Senior Advisor Innovation and the Civil Aviation Authority's Chief Legal Counsel. The Project Initiation Document containing a general description of the Project was supplied to , and supplementary information was provided in response to specific questions about the Trial and the Project.

Drafts of the PIA were provided by and comments were received from the Office the Privacy Commissioner on 15 June 2020. Further drafts were prepared, and another draft forwarded to the Office of the Privacy Commissioner on [21/08/2020]. The PIA was reviewed and approved by [*Gordon Davis Chief Legal Counsel AVSEC/CAA*] on [*21/08/2020*].

The Privacy Impact Assessment was prepared under the Privacy Act 1993, however, there have been no substantial changes to the Assessment resulting from the 2020 Privacy Act.

We have reviewed the Privacy Impact Assessment in this light and have updated the reference to reflect the provisions under the new Privacy Act 2020. Otherwise, the Assessment remains the same

2.3 The rationale for the PIA

The Trial and Project will involve the collection of matching datasets of passengers and non-passengers passing through airport security screening areas. The collection of matching datasets involves the collection of personal information, identifying information about an individual, under the Privacy Act 2020.

AVSEC was concerned to ensure that from the outset the Trial and Project had full regard to the information privacy principles contained in the Privacy Act 2020.

The PIA was an opportunity for AVSEC to obtain an independent review of the design of the Trial and Project to ensure that all relevant privacy implications were identified and considered.

3. Personal information

The matching dataset obtained from a passenger and non-passenger passing through the security screening area is personal information under the Privacy Act 2020, as it is information that is capable of identifying a living human being.

Key terms used in this PIA

Digital signature:	an image which has been converted to a string of numbers or encrypted datasets of the image.
Matching dataset:	a digital signature that is produced using encryption [redacted] software from an image from the video feed of a passenger or non-passenger entering and exiting a security screening area
Recognition dataset:	a digital signature that is produced using encryption [redacted] software from a digital photo image of an AIC holder from the AIC database

The Trial involves the installation of cameras at an AVSEC security screening area that will allow the use of [redacted] recognition software to count persons (passengers and non-passengers) passing through the security screening area, and to determine the wait time for the security screening services experienced by each passenger.

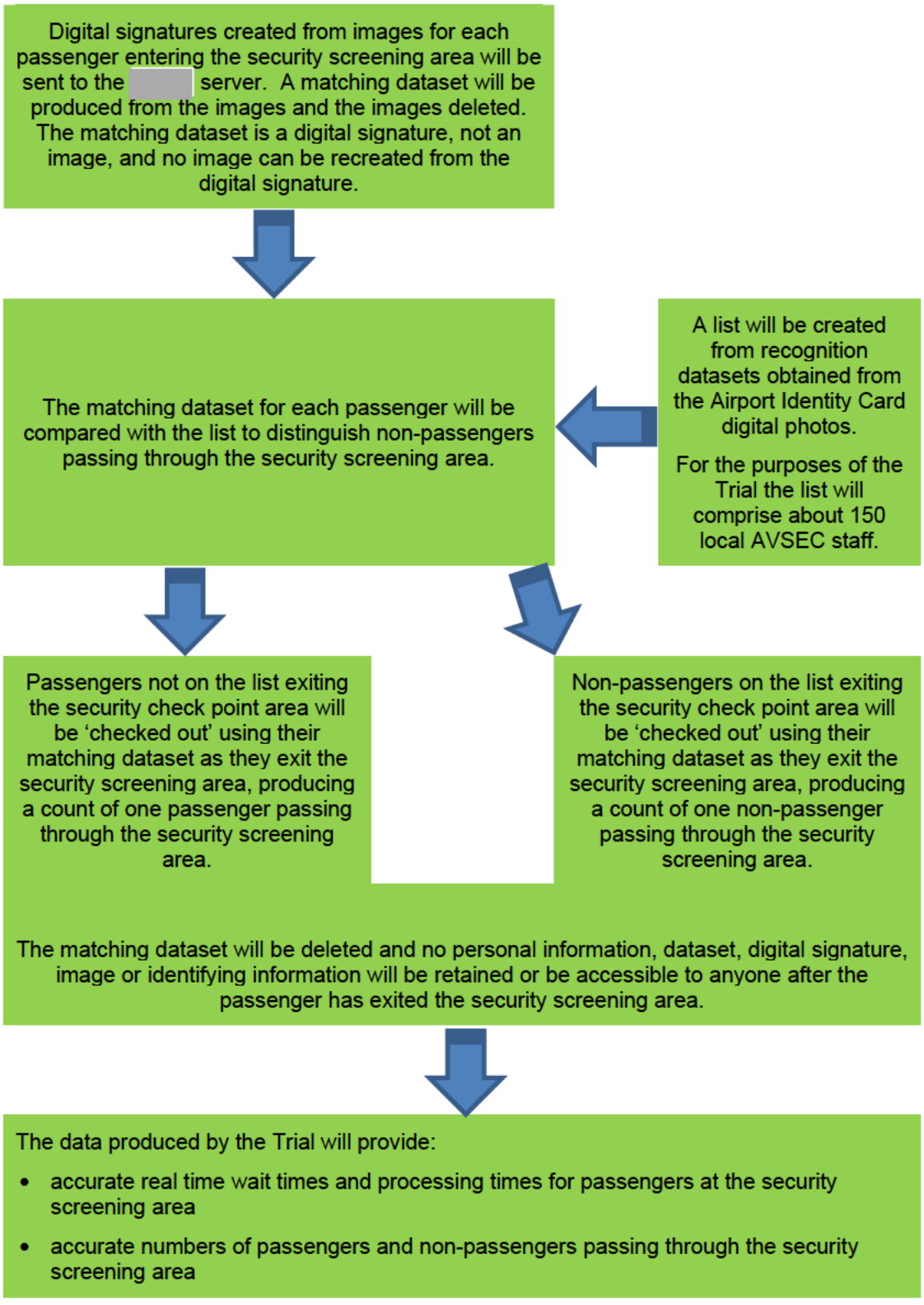
Cameras will initially capture images of passengers and non-passengers entering the queue at the screening area. The stream of images will be transmitted to the [redacted]. The facial image will be converted into a digital signature that comprises a unique string of numbers or encrypted datasets of the image.

The images will not be retained, as once the digital signatures are created, no further use will be made of it. Only datasets, comprising the digital signatures of passengers

and non-passengers, will be held in a temporary database on the server. The datasets will be stored on a hard drive and will also be retained in a temporary memory cache that operates like RAM (random access memory) while the passenger or non-passenger transits the screening area.

The datasets will be held on the hard drive and in the temporary memory cache only while the passenger or non-passenger is passing through the security screening area. Once the person exits the queue and is matched against the dataset of their entry to the queue, the dataset will be deleted by the database and the memory cache. This deletion will occur 20 minutes after the dataset was created. Thus, the retention of the dataset, which is only a digital signature comprising numbers and not an image, will only be very temporary and held only for 20 minutes. No other use will be made of the digital signature. The digital signature will only be used to count the number of passengers passing through the security screening area.

The information flows for the Trial are set out in the diagram below.



3.1 Collection and use of matching data

The matching dataset of each passenger will only be used for the purpose of counting each passenger passing through a security screening area. The matching dataset will be encrypted and only held temporarily in a memory cache while the passenger or non-passenger is passing through a security screening area and then deleted.

The Trial and Project will produce a tally of the total number of passengers and non-passengers who pass through a security screening area. If a person enters a security screening area, but there is no match for that person exiting the security screening area, for example, because the video image is not of sufficient quality to produce an accurate digital signature, there will be no count of that person passing through the security screening area.

Collection of information from AIC database

Initially, for the Project, the recognition dataset for each of the 150 AVSEC personnel participating in the Trial will be obtained from the AIC database[1]. The AIC database is held by a separate group within AVSEC and contains photos of all people who have an AIC. The AIC photo for each Trial participant will be given a unique identifier (most likely an individual number) by the AIC database and forwarded to the [redacted] server. The [redacted] software will generate a recognition dataset for each AIC photo. The unique identifier will enable the AIC information system to ensure the recognition datasets are kept up to date and a dataset deleted when a person leaves AVSEC and no longer has an AIC. The recognition dataset will be held on the [redacted] server as a digital signature, not an image, and no image can be recreated from that dataset. The AIC photo will be held on the [redacted] for the duration of the Trial.

AVSEC staff managing the Trial and Project will only be able to determine that a person has entered a security screening area, that the person may or may not have been identified as a list entity, and that the person has checked out of the security screening area. AVSEC airport staff will have no access to, or information about, the identity of any person or list entity (passenger or non-passenger) and no ability to access any image of the person.

The collection of recognition datasets from the AIC database for the implementation of the Project is proposed to be different. For the Project there will be no manual collection of information from the AIC database. Instead, the collection of digital signatures will be automated by the regular scheduled importation of images from the AIC database into [redacted] to allow [redacted] to generate and store the digital signatures for live image matching. This will ensure the recognition datasets from the AIC database are always up to date and there are no matches to AIC holders that are no longer valid, for example, from an AIC holder passing through a security screening area with an expired AIC.

[1] All people who enter a security area at an airport are required under rule 19.357(b) of the Civil Aviation Rules 1990 to have an AIC, although there are a number of specific exceptions in the Rules to this requirement.

3.2 Accuracy of recognition technology software

Some recognition technology software has been criticised for racial and gender bias. However, the use of recognition software in the Trial and Project will not raise any issues of racial or gender bais because the software is only being used to differentiate passengers from non-passengers and to determine whether a person who entered the queue has exited the queue.

The [redacted] software is subject to regular independent National Institute of Standards and Technology testing and scores very highly in its ability to accurately identify faces across a range of racial and gender groups.[2] As noted above, the performance and accuracy of the [redacted] software is not directly relevant to its use for the Project as the Project is only seeking a match in order to count a passenger passing through a security area. A failure of the software to properly identify a match simply results in one less count of a passenger or non-passenger, not in the selection of a person using some sort of criteria that is subject to racial or gender bias. In the context of the 0.003% failure rate of the software to match faces[3] the effect of any failure to count a passenger or non-passenger will be negligible. Unlike other uses of recognition software where a person is being profiled for further observation, investigation, or enforcement action, a failure to count a passenger or non-passenger has no consequences for the passenger or non-passenger.

2 '[redacted] Facial Recognition NIST Report Analysis – January 2020" [redacted], 28 June 2020.

3 Above note 2 at page 4.

3.3 Trial cameras

AVSEC currently operates and obtains CCTV footage of people moving through security screening areas at airports. The existing CCTV cameras at the security screening areas are visible to people moving through those areas. The CCTV footage is used for incident investigation, duress alarms, complaint resolution, security detection and video surveillance at the Operations Centre control room. However, the current CCTV cameras are not capable of supporting the data transfer speeds to a cloud-based system that are fast enough for real time recognition analytics.

New edge cameras will be installed for the Trial and they will also be visible to people moving through the security screening areas.

The cameras will stream images of passengers, which will be stored temporarily to allow the creation of digital signatures, and then the video images and digital signatures will be deleted after the digital signatures have been used for matching. No other body images or carried items will be recorded.

There will be no audio recording of people moving through the security screening areas.

3.4 Storage and retention of matching data

The matching dataset obtained from a passenger entering a security screening area will be held in a temporary memory cache on the server to be matched with the matching dataset of the same passenger exiting the screening point area. Each match will produce a count of one passenger passing through the security screening area. If the person is a list entity the system will produce a count of one non-passenger passing through the security screening area.

A risk assessment on the server and Controls Validation Assessment has been undertaken and a "Certification and Accreditation Memorandum" signed by the Executive Group Manager, the Chief Information Officer and the Security Officer of the Authority certifying that all applicable controls for the handling and management of personal information have been satisfied.

The video feed from the cameras at the security screening area will not be held on the server after the digital signatures have been generated.

No matching datasets obtained from passengers entering and exiting the security screening area will be retained on the server for longer than twenty minutes. For the Trial, recognition datasets of AIC holders will be held on the server, but for the Project these datasets will be accessed directly by the server and no recognition datasets will be held on the server.

3.5 Consent of Trial participants

Travelling passengers will be advised of the operation of the Trial. Notices will be placed at the entrance to the security screening area advising passengers that recognition technology will be used to count them as they pass through the security screening area. The notice will inform passengers of the collection of the recognition dataset, the purpose of the collection of the information, the use of recognition technology to 'count' them as they pass through the security screening area, and provide contact information for AVSEC. A sample of the proposed notice to passengers is attached as an Appendix.

For those AVSEC staff participating in the Trial consent was obtained to use their images from the AIC information system for populating the list for the purposes of the Trial.

3.6 Benefits of Trial/ Project

Queue wait times are currently calculated manually on a sample only basis by a data analyst viewing CCTV footage. The wait times provide poor quality data as the results are inaccurate and inconsistent. The wait times are also inefficient and labour intensive to produce.

Improved data on wait times is critical to enable AVSEC to accurately identify the services it provides to passengers and non-passengers (as only the former pay the Aviation Security Service levy).

The Trial might also provide AVSEC with reliable data for calculating accurate service levels of performance for security checkpoint staffing and resourcing.

The wait times and data will be able to be 'sliced and diced' as needed to produce data for different time periods.

Accurate information on wait times might also provide AVSEC with information that will enable it to better manage queues and wait times at security screening areas through better allocation of resources and by providing real time information to passengers about wait times.

4. Other options considered

Over the last 3 years AVSEC have considered and explored a number of other options for counting passengers passing through security screening areas. At least three alternative solutions were investigated and particular products for each of those solutions were trialled. Possible options considered included –

Investigation of the use of IOT sensors, which make use of movement to count people going through a given area. The investigation involved the demonstration of a particular product solution. IOT sensors can provide a 98% accuracy rate for people counts, but do not provide the benefits of segregating counts for a particular purpose, giving only a total count of all people within a given radius. IOT sensors are not capable of providing accurate passenger wait times.

The use of Bluetooth or Wi-Fi trackers, however these can only count about 30-40% of passengers. The investigation involved the demonstration of a particular product solution and conversations with airport companies that are using this technology for counting people. Bluetooth or Wi-Fi trackers cannot count passengers whose phones or wearable trackers are switched off or on flight mode, and passengers without Bluetooth or Wi-Fi enabled devices will not be counted, such as children and elderly people. Bluetooth or Wi-Fi trackers will produce unrepresentative passenger wait times given the low percentage of participants.

CCTV counting solutions were considered, which give a total count of people going past a certain point, but there is no ability to separate groups going through and the CCTV solutions will not give passenger wait times. Again, a number of particular products were investigated and demonstrated.

5. Privacy assessment

Each row in the following table summarises the key requirements of each of the information privacy principles (contained in s 22 of the Privacy Act 2020 and available here) and identifies any key issues or considerations that should be addressed.

#	Description of the privacy principle	Summary of personal information involved, use and process to manage	Assessment of compliance
1	Principle 1 - Purpose of the collection of personal information Only collect personal information if you really need it	The collection of matching datasets and recognition datasets from passengers and non-passengers forms the essence of the Trial/ Project. Counting passengers and non-passengers using AVSEC's security screening service in order to display the wait time for that service and accurately calculate the Aviation Security Service levy is part of the efficient administration and provision of security services required by s 80 and Part 8 of the Civil Aviation Act 1990. The matching data enables the Trial/ Project to 'count' passengers and non-passengers efficiently, accurately and in an unobtrusive way. The use of matching and recognition datasets was the only option that would produce accurate counts and wait times for passengers.	**Collection of matching datasets complies** The collection of matching and recognition datasets of passengers and non-passengers for the Trial/ Project is connected with a lawful purpose of AVSEC and necessary for that purpose. A number of other options were considered but none of the options were able to count passengers, separate out AIC holders and provide wait times [see Section 4 above for more details of the options considered].

2	Principle 2 – Source of personal information Get it directly from the people concerned wherever possible The relevant parts of Principle 2 are: *(1) Where an agency collects personal information, the agency shall collect the information directly from the individual concerned.* *(2) It is not necessary for an agency to comply with subclause (1) if the agency believes, on reasonable grounds,—* *…* *(a) that non-compliance would not prejudice the interests of the individual concerned; or* *(c) that the individual concerned authorises collection of the information from someone else; or* *…* *(g) that the information—* *(i) will not be used in a form in which the individual concerned is identified; or* *(ii) will be used for statistical or research purposes and will not be published in a form that could reasonably be expected to identify the individual concerned; or …*	**Matching dataset** The matching dataset is collected directly from people entering the security screening area. **Recognition dataset** The collection of the recognition datasets for the Trial from the AIC database will be authorised by each AIC holder. The alternative would require each AIC holder to have their identity verified each time they pass through the security screening area and would be more intrusive. The collection of recognition datasets from the AIC database will – • be authorised by an AIC holder • not be used in a form in which the AIC holder passing through the security screening area will be identified • be used for statistical purposes and not be published in a form that could identify an AIC holder • not prejudice the interests of an AIC holder	**Collection of matching datasets complies** The collection of matching datasets directly from people entering the security screening area for the Trial/ Project will comply with Principle 2. **Collection of recognition datasets satisfies at least one or more of the following four exceptions to compliance** The collection of recognition datasets from the AIC database for the Trial does not comply with Principle 2, which requires collection directly from the individual AIC holder. As noted, collection of the recognition dataset directly from the AIC holder would require verification of the identity of the AIC holder each time they passed through a security screening are and would be more intrusive. However, the collection of the recognition dataset will be authorised by the AIC holder and satisfy the exception in Principle 2(2)(c). Further, at least one or more of the following three exceptions to compliance apply – • the recognition dataset "will not be used in a form in which the [AIC holder] is identified" – Principle 2(2)(g)(i). The video feed will produce a count of an AIC holder passing through the security screening area, but neither the matching of a recognition dataset with a matching dataset, nor the resulting

#	Description of the privacy principle	Summary of personal information involved, use and process to manage	Assessment of compliance
			count use personal information, as they will not identify an AIC holder. The datasets only contain numbers. There are no images in the datasets, and no images can be recreated from the datasets; • the recognition dataset "will be used for statistical purposes and will not be published in a form that could reasonably be expected to identify the [AIC holder]" – Principle 2(2)(g)(ii). The video feed will produce a count of an AIC holder passing through the security screening area, but neither the matching of a recognition dataset with a matching dataset, nor the resulting count, will identify an AIC holder; • non-compliance "will not prejudice the interests of the [AIC holder]" – Principle 2(2)(a). Given the use of a recognition dataset will be to produce a statistical result that will not identify an AIC holder, an AIC holder will not be prejudiced in any way.

3	Principle 3 – Collection of information from subject Tell them what information you are collecting, what you're going to do with it, whether it's voluntary, and the consequences if they don't provide it.	**Matching dataset** Passengers entering the security screening area will be advised of the general terms of the Trial, and the use of recognition technology to 'count' them as they pass through the security screening area [See Section 3.5 above and the Appendix]. The matching dataset will – • not be used in a form in which the passenger will be identified • will be used for statistical purposes and the information will not be published in a form that could identify the passenger • will not prejudice the interests of the passenger. **Recognition dataset** AVSEC will seek the consent of an AIC holder to the collection and use of the recognition dataset (their AIC photo) for the purposes of the Trial, and AVSEC will advise an AIC holder of the features of the Trial in accordance with the requirements of Principle 3(1).	**Collection of matching dataset from passenger does not comply** The collection of matching datasets from people entering the security screening area for the Trial will not comply with Principle 3(1). However, at least one or more of the following three exceptions to compliance are considered to apply – • the matching dataset will not be used in a form in which the passenger will be identified – Principle 3(4)(e)(i). The video feed will produce a count of a passenger passing through a security screening area, but neither the matching dataset, nor the resulting count use personal information, as they will not identify a passenger. The datasets only contain numbers. There are no images in the datasets, and no images can be recreated from the datasets; • the matching dataset will be used for statistical purposes and the information will not be published in a form that could identify the passenger – Principle 3(4)(e)(ii) . The video feed will produce a statistical count of a passenger passing through a security screening area, but neither the matching dataset, nor the count use personal information, as they will not identify a passenger. The datasets only contain numbers. There are no images in the datasets, and no images can be

#	Description of the privacy principle	Summary of personal information involved, use and process to manage	Assessment of compliance
			recreated from the datasets; • non-compliance will not prejudice the interests of the passenger – Principle 3(4)(a). Given the use of a recognition dataset will be to produce a statistical result that will not identify a passenger, the passenger will not be prejudiced in any way. **Collection of recognition dataset from AIC holder complies** The collection of recognition datasets from an AIC holder entering the security screening area for the Trial/ Project will comply with Principle 3(1). In addition, at least one of the three exceptions to compliance noted in the bullet points above are considered to also apply to an AIC holder as they apply to a passenger.

#	Description of the privacy principle	Summary of personal information involved, use and process to manage	Assessment of compliance
4	Principle 4 – Manner of collection of personal information Be fair and not overly intrusive in how you collect the information	The matching datasets will be collected by cameras mounted around the walls and roof of the security screening area. The cameras will be fully visible to all people entering the security screening area. Passengers entering the security screening area will be advised of the purpose of the cameras and the way in which the cameras will be used [See also Section 3.5 above, Principle 3 above, and the Appendix].	**Manner of collection complies** The manner of collection of the matching datasets for the Trial/ Project will comply with Principle 4. The use of recognition software will count the passengers through the security screening area but no identifying information of passengers will be used or retained. Passengers will be advised of the purpose and use of the cameras in the screening area, which is a high security area. Passengers have a lower expectation of privacy in security screening areas, which include CCTV cameras where passengers are advised they are entering a security area where they are required to submit their bags to screening and may themselves be searched for prohibited items. Given the use of the cameras will be to count passengers and no identifying information about a passenger will be retained after the passenger exits the screening area it is considered the use of the cameras to create matching datasets would not be considered by passengers to be unfair or to intrude to an unreasonable extent upon the personal affairs of passengers – Principle 4(b)(i) and (ii).

#	Description of the privacy principle	Summary of personal information involved, use and process to manage	Assessment of compliance
5	Principle 5 – Storage and security of personal information Take care of it once you've got it and protect it against loss, unauthorised access, use, modification or disclosure and other misuse.	The storage and security of the matching datasets and recognition datasets has been subject to a separate "Security Review" by [redacted]	A "Certification and Accreditation Memorandum" is in place signed by the Executive Group Manager, the Chief Information Officer and the Security Officer of the CAA certifying that all applicable controls for the handling and management of personal information have been satisfied.

#	Description of the privacy principle	Summary of personal information involved, use and process to manage	Assessment of compliance
6	Principle 6 – Access to personal information People can see their personal information if they want to Note that this principle only applies if the personal information is held "in such a way that it can readily be retrieved".	**Matching dataset** The matching datasets are held as datasets for each person who enters the security screening area. There is no identifying information that will enable a person to request access to a particular dataset, as no name, date of birth or other identifying feature will be associated with the matching dataset. As the datasets will only be held for the duration the person is in the security screening queue there will be little or no opportunity for a passenger to request access to their dataset. The datasets will be held for a fixed period of 20 minutes, to allow for queues of up to that length of time. **Recognition dataset** An AIC holder will be able to request access to their recognition dataset via a request attaching a digital photo of themselves to be matched with the recognition dataset.	**A passenger will not be able to access their matching dataset as it will not be readily retrievable** Principle 6 must be read with Subparts 1 and 2 of Part 4 of the Privacy Act 2020, which set out the procedural provisions for accessing and correcting personal information. Section 44(2)(a) of the Privacy Act 2020 provides that it is a good reason to refuse access to personal information if that information is not readily retrievable. Principle 6 does not apply to the Trial/ Project as the matching datasets will not be readily retrievable. The matching datasets will only be held while the passenger is in the security screening queue and then will be deleted, meaning there will be no opportunity for a person to access their matching dataset. **Recognition dataset** An AIC holder will be able to request access to their recognition dataset and this will comply with Principle 6.

#	Description of the privacy principle	Summary of personal information involved, use and process to manage	Assessment of compliance
7	Principle 7 – Correction of personal information They can correct it if it's wrong, or have a statement of correction attached	**Matching dataset** Principle 7 is not applicable to passengers as it only applies if a person can access their personal information under Principle 6. **Recognition dataset** An AIC holder will be able to request correction of a recognition dataset, although it is unlikely this principle will ever apply given there would be no grounds for an AIC holder to request a correction to a photo.	**Not applicable to passengers** Principle 7 is not applicable to passengers in respect of the Trial/ Project. **Recognition dataset** An AIC holder will be able to request a correction to their recognition dataset and this will comply with Principle 7.
8	Principle 8 – Accuracy etc. of personal information to be checked before use Make sure personal information is correct, relevant and up to date before you use it	The nature of the personal information at issue here – a digital rendering of a person's face that is taken at the time the person enters the security screening area – means the personal information being collected will always be accurate, up to date, complete and not misleading in any way. For a discussion of bias and recognition technology and why it doesn't affect the Trial see Section 3.2 above.	**Complies** The Trial/ Project will comply with Principle 8.

#	Description of the privacy principle	Summary of personal information involved, use and process to manage	Assessment of compliance
9	Principle 9 – Not to keep personal information for longer than necessary Get rid of it once you're done with it	The image feed from the cameras at the security screening area will not be held on the [redacted] after the digital signatures have been generated from the video feed images. **Matching dataset** The matching datasets will only be kept in a temporary memory cache for twenty minutes while a passenger is in the security screening queue and then the dataset will be deleted. **Recognition dataset** The AIC photos and recognition datasets will be retained on the [redacted] server for the duration of the Trial and then deleted.	The non-retention of the image feed after the digital signatures have been generated from the images on the video feed will comply with Principle 9 as the imagefeed will not be kept for any longer than necessary. **Retention of matching dataset complies** The matching datasets will only be kept very temporarily in a memory cache while a passenger is in the security screening queue and then deleted. This is no longer than necessary and complies with Principle 9. **Retention of recognition dataset complies** The AIC photos and recognition datasets are required for the duration of the Trial and their deletion at the end of the Trial will ensure they are not retained for longer than is necessary.

#	Description of the privacy principle	Summary of personal information involved, use and process to manage	Assessment of compliance
10	Principle 10 – Limits on use of personal information Use it for the purpose you collected it for, unless one of the exceptions applies	**Matching dataset** The matching datasets will only be used for the purpose for which they were collected – 'counting' the person through the security screening area, as advised to the passenger in accordance with Principle 3. **Recognition dataset** The recognition datasets will only be used for the purpose for which they were collected from the AIC database, as consented to by an AIC holder – matching with the matching datasets of AIC holder's passing through the security screening area to distinguish AIC holders from passengers.	**Complies** The use of the matching datasets and recognition datasets for the Trial/ Project will comply with the limits in Principle 10 as they will only be used for the purpose of counting passengers and non-passengers through a security screening area.
11	Principle 11 – Limits on disclosure of personal information Only disclose it if you've got a good reason, unless one of the exceptions applies	No disclosure of the matching datasets or the recognition datasets will occur during the Trial or Project.	**Complies** The Trial and Project will comply with the limits on disclosure in Principle 11.
12.	Principle 12 – Limits on Cross-border disclosure Only disclose personal information to an entity outside of New Zealand in certain circumstances	Principle 12 is not applicable to the Trial or the Project. Neither the matching datasets nor the recognition datasets will be disclosed to any other entity either inside or outside of New Zealand.	**Complies** The use of the matching datasets and recognition datasets for the Trial/ Project will comply with Principle 12 as they will only be used for the purpose of counting passengers and non-passengers through a security screening area.

#	Description of the privacy principle	Summary of personal information involved, use and process to manage	Assessment of compliance
13	Principle 13 – Unique identifiers Only assign unique identifiers where permitted	**Matching dataset** Unique identifiers will not be assigned to the matching datasets, or to the extent unique identifiers are assigned, they will not allow anyone within the Trial or Project to identify a person. **Recognition dataset** Numbers or some other form of unique identifier will be assigned to the recognition datasets by the AIC database before the datasets are provided to the Trial/ Project. The unique identifiers will enable the AIC database to update, amend, delete etc the datasets to ensure they remain accurate and up to date. However, those unique identifiers will be attached to a digital signature that does not identify the AIC holder. Neither the digital signature nor the unique identifier will allow the Trial/ Project to link the digital signature or unique identifier back to an identifiable person.	**Complies** The Trial will comply with Principle 13 as unique identifiers will not be assigned to the matching datasets or recognition datasets, or to the extent that unique identifiers are assigned, they will not be capable of being linked back to an identifiable person.

5.1 Summary / Conclusions

The above analysis of the compliance of the Trial with the information privacy principles contained in the Privacy Act 2020 shows that the Trial will comply with the information privacy principles.

Collection of the recognition datasets from the AIC database and not from the AIC holder

Principle 2 requires the collection of personal information directly from the person concerned. The collection of the recognition datasets from the AIC database and not from the AIC holder does not comply with Principle 2.

It is considered that requiring compliance with Principle 2 would be more intrusive than not complying. If the recognition dataset were to be collected from an AIC holder the AIC holder would have to have their identification verified each time they passed through a security screening area. By obtaining the consent of an AIC holder to use their AIC photo from the AIC database (in accordance with the exception in Principle 2(2)(c)) there will be no need to verify the identity of an AIC holder passing through a security screening area.

In addition, the collection of the recognition datasets from the AIC database will satisfy at least one or more of the following exceptions in Principle 2(2)(c) and (g)(i) and (ii):

- the recognition datasets will not be used in a form in which an AIC holder will be identified – Principle 3(4)(e)(i);
- the datasets will be used for statistical purposes and the information will not be published in a form that could identify an AIC holder – Principle 3(4)(e)(ii); and
- the collection of a recognition dataset will not prejudice the interests of an AIC holder – Principle 3(4)(a).

The video feed from the security screening area will produce a count of an AIC holder passing through the security screening area, but neither the matching of a recognition dataset with a matching dataset, nor the resulting count use personal information, as they will not identify an AIC holder. The datasets only contain numbers. There are no images in the datasets, and no images can be recreated from the datasets.

Given the use of a recognition dataset will be to produce a statistical result that does not identify an AIC holder, it is not considered that an AIC holder will be prejudiced in any way.

Passengers will not be fully informed of the collection of the matching dataset

Principle 3 requires people to be told what information you are collecting, what you're going to do with it, whether it's voluntary, and the consequences if they don't provide it. The Trial will not fully inform passengers of the collection of the matching dataset and does not comply with Principle 3, but will be saved by one or more of the exceptions to compliance. For example:

- a matching dataset will not be used in a form in which a passenger will be identified – Principle 3(4)(e)(i);

- the datasets will be used for statistical purposes and the information will not be published in a form that could identify a passenger – Principle 3(4)(e)(ii); and
- non-compliance will not prejudice the interests of a passenger – Principle 3(4)(a).

The video feed will produce a count of a passenger passing through a security screening area, but neither the matching dataset, nor the resulting count use personal information, as they will not identify a passenger. The datasets only contain numbers. There are no images in the datasets, and no images can be recreated from the datasets.

Given the use of a recognition dataset will be to produce a statistical result that will not identify a passenger, it is not considered that a passenger will be prejudiced in any way.

However, in addition to the application of the above exceptions, AVSEC intends to inform passengers of the collection of the recognition dataset, the purpose of the collection of the information, the use of recognition technology to 'count' them as they pass through the security screening area, and provide contact information for AVSEC. A sample notice to passengers is attached as an Appendix.

Passengers will not be able to have access to their matching dataset because it is not readily available

Principle 6 requires people to have access to their personal information if they want to. The matching datasets will only be held in a temporary memory cache for the duration the person is in the security screening queue so there is little or no opportunity for a passenger to request access to their dataset.

Section 44(2)(a) of the Privacy Act 2020 provides that it is a good reason to refuse access to personal information if that information is not readily retrievable. Therefore, Principle 6 does not apply to persons requesting access to their matching dataset as it will not in practice be readily retrievable.

An AIC holder will be able to request access to their recognition dataset via a request attaching a digital photo of themselves to be matched with the recognition dataset.

AIC Project participants

The extension of the Project to include a much wider range of AIC holders (such as all AVSEC staff, airport company staff, border control agency staff (Customs, Immigration New Zealand, New Zealand Police), airline ground crew, and aircrew (international and domestic)) will raise new issues that will need to be further considered during the design stages of the Project. For example, issues may arise in respect of the collection of recognition datasets from those non-passengers who do not have an AIC, and the period of retention of those datasets.

Important note: this assessment of compliance is based on the terms of the Trial and Project as set out in this PIA

The assessment of the compliance of the Trial, and where known, the terms of the proposed Trial, is based on the terms of the Trial and Project as set out in this PIA. Some of those terms are critical to the conclusions regarding compliance. For example, the inability of AVSEC staff managing the Trial and Project to access identifying information about AIC holders is critical to the conclusions regarding the collection and use of the AIC matching datasets.

Any changes to the terms of the Trial or Project need to be reassessed for their potential impact on the compliance of the Trial or Project with the information privacy principles.

6. Risk assessment

The risks associated with the Trial and Project arise not from the way the Trial or Project will operate, but from the potential generation of a temporary recognition database of people passing through security screening areas at airports in New Zealand.

The risks have been grouped into four different types of risk:

- **Risk 1: An alert system for other enforcement agencies** – the use by other enforcement agencies of the recognition capability as an alert system to identify particular persons passing through security screening areas at airports.
- **Risk 2: A tool to monitor AIC card holders** – the use of the recognition capability to monitor the movement of AIC card holders through airport security areas;
- **Risk 3: Breach of internal security controls** – AVSEC staff/ contractors managing the Trial/ Project obtain access to identifying information about the AIC recognition datasets;
- **Risk 4: A Facial Recognition database** – a temporary database with recognition capability for people passing through security screening areas at airports in New Zealand.

Each of these risks are discussed in more detail below.

Risk 1: An alert system for other enforcement agencies

The matching datasets could potentially be used by other enforcement agencies as an alert system to identify particular persons passing through security screening areas at airports.

A number of key controls have been identified to ensure this risk is eliminated. First, the [redacted] software ID Gateway solution will be written so that it will only accept images provided by the video feeds from the cameras at the security screening areas. There will no ability for a third party, such an enforcement agency, to seek information about a match between a digital signature they possess and a passenger passing through a security screening area, as the solution will not accept any inputs other than from the video feeds at AVSEC security screening areas.

Secondly, the matching datasets of passengers and non-passengers passing through a security screening area will only be kept for as long as necessary – that is the time the passenger or AIC holder is in the security screening queue and will be set at twenty minutes. This ensures that no database of matching datasets will exist that could be the subject of a subsequent request by an enforcement agency. The matching dataset will be created in a temporary memory cache as a passenger enters the queue and will be deleted twenty minutes later.

Thirdly, there is no usable database that an enforcement agency can obtain access to or 'uplift' pursuant to a court order. This is because the [redacted] software is encrypted so a request to access recognition datasets cannot be actioned without the [redacted] encryption key. Any enforcement agency seeking information about a matching

dataset would need to compel AVSEC to produce the electronic key to obtain access to the [redacted] software.

Risk 2: A tool to monitor AIC card holders

The Trial and Project have the potential to monitor the movements of all AIC card holders. It is assumed that this potential exists at present in respect of the security screening areas where AIC holders are required to show their card but would require details of the AIC holder to be recorded. The Trial and Project will make this process of tracking the movements of AIC holders much simpler by enabling their movements to be continuously monitored as they enter and exit security screening areas. A large traceable record could potentially be generated of all the movements of AIC holders.

The ability to unobtrusively monitor all AIC holders may make it attractive for some of the employers of AIC holders to obtain the consent of their employees and contractors to obtain further information about the movements of their staff. The likelihood of this happening will increase as the scope of the Project increases. It is proposed that the Project will apply to a much wider range of AIC holders than the Trial. The Project will be broadened to include all AVSEC staff, airport company staff, border control agency staff (Customs, Immigration New Zealand, New Zealand Police), airline ground crew, and aircrew (international and domestic).

However, the purpose of the AIC system is to manage security at airports. The use of the recognition datasets to identify the movement of AIC holders for purposes that are not security related will be inconsistent with the information privacy principles in the Privacy Act 2020, is likely to undermine the integrity of the AIC airport security system, as well as be inconsistent with the purpose of the AIC system under the Civil Aviation Rules 1990.

This risk will be eliminated because there will be no traceable record of the movements of AIC holders, and the matching datasets of AIC holders passing through security screening areas will only be retained for the minimum time period they are required (the duration of the AIC holder's passage through the security screening area). AVSEC will not hold records of AIC holders passing through the security screening areas and it will not be able to respond to requests for information about the movement of employees and contractors through the security screening areas even if those employees have consented to the release of such information.

Risk 3: Breach or lapse of internal security controls

The compliance of the collection and use of the matching dataset from the AIC database is dependent on those matching datasets not containing any information that would identify the individual AIC holder. Access by AVSEC staff and contractors to the AIC database is currently limited by internal AVSEC controls. Any breach, oversight, error, or lapse in those controls could allow AVSEC staff or contractors access to identifying information about the matching datasets of AIC holders. It is important for the compliance of the Trial and Project that those internal security controls that have been reviewed by the Security Review are maintained and adhered to.

Risk 4: A Facial recognition database

The largest risk to the Trial and to the Project, but also the easiest risk to eliminate, is the potential for the Trial and Project to create a database with recognition capability in respect of people passing through security screening areas at airports in New Zealand. Such a database held by a government agency would be controversial for all airport users if the database was developed without their knowledge and without a clearly limited purpose.

This risk is most easily eliminated by ensuring that the matching datasets of everyone passing through a security screening area are only kept for as long as the necessary – that is the time the passenger or AIC holder is in the security screening queue, which will be set at twenty minutes. This will ensure that no database with recognition capability will ever exist. The matching dataset which will be created in a temporary memory cache as a passenger enters the queue will be deleted twenty minutes later.

7. Recommendations to minimise impact on privacy

The following recommendations are intended to mitigate the risks identified in the previous section.

Ref	Recommendation	Agreed Yes/ No
R-001	The [redacted] software is written to allow inputs of images only from the cameras located in the AVSEC security screening areas so there will no ability for a third party, such an enforcement agency, to seek information about a match between a digital signature they possess and a passenger passing through a security screening area. The matching datasets of passengers passing through a security screening area be kept only for as long as necessary – that is the time the passenger is in the security screening queue, which will be set at twenty minutes. This will ensure that no database of matching datasets will exist that could be the subject of a request by an enforcement agency. The [redacted] software uses encryption so a request to access recognition datasets cannot be actioned without an encryption key.	Agreed
R-002	No record of the movements of AIC holders is generated or retained by the Trial or Project.	Agreed
R-003	AVSEC's internal controls that prevent access by AVSEC staff and contractors to the AIC database are considered adequate to prevent any breach, oversight, error, or lapse that could allow AVSEC staff or contractors access to identifying information about the matching datasets of AIC holders.	Agreed
R-004	The matching datasets of anyone passing through a security screening area are only kept for as long as necessary – that is the time the passenger or AIC holder is in the security screening queue and set at twenty minutes.	Agreed

Appendix – Privacy Notice

Use of recognition-based technology to count passengers using the security screening service

The purpose of this notice is to advise you of the trial of recognition technology to count the number of passengers using the security screening service and to produce a wait time for the security screening service so passengers know how long they can expect to wait in the queue.

What personal information is being collected?

Cameras will capture an image from a video feed of you entering the security screening queue. The face biometric data from the image will be converted to a digital signature (numbers) and the image deleted.

The digital signature is retained in a temporary memory cache in a secure government dedicated server only for the duration that you are in the queue. When you exit the queue another camera records your exit, creates another digital signature and matches your exit with the digital signature of your entry.

Why is this information being collected?

The information will be used to compile a wait time that is displayed for other passengers so they know how long they can expect to wait in the queue, and produce a count of the number of passengers using the security screening service.

What information is stored?

The images of your entry and exit are deleted after the digital signatures have been created, and the digital signatures are then deleted after you exit the queue. No other use is made of the video feed or digital signature other than to count the number of passengers passing through the security screening area.

There is no image or digital signature retained of the fact that you have used the security screening service.

What information can you access?

As no image or digital signature of you is retained after you have exited the queue there is no personal information retained that you can request access to, or correction of.

Who authorised the collection of this information?

The collection of this information is authorised by the Aviation Security Service in order to:

- provide passengers with better information about the wait time at the security screening area;
- count the number of passengers using the security screening service.

Further information about this Trial

This queue counting and wait time service is provided by the Aviation Security Service, the certified aviation security service operator at designated airports. The contact details for the Aviation Security Service in respect of this Trial are:

The Privacy Officer
Aviation Security Service
PO Box 3555
Wellington 6140
Email: timetrial@avsec.govt.nz