Te Pā Whakamarumaru
New Zealand Security Intelligence Service

Electronic Travel Authority (ETA) Data

and

Advance Passenger Processing (APP) Data

PRIVACY IMPACT ASSESSMENT

Owner	Knowledge Manager
Approved By	Chief Privacy Officer
Approval Date	7 December 2025
Review Date	7 December 2028

Contents

Part 1: Relevant Legislation

1. Under section 125(1) and Schedule 2 of the Intelligence and Security Act 2017 (**ISA**), the New Zealand Security Intelligence Service (**NZSIS**) is authorised to have direct access to certain information held by other agencies.

2. The direct access agreement between the Minister responsible for NZSIS and the Minister responsible for Immigration came into effect on 7 December 2025 after being signed by both parties (**DAA**) and enables NZSIS to access Electronic Travel Authority (**ETA**) data and Advance Passenger Processing (**APP**) data collected by Immigration New Zealand (**INZ**)[1] under the Immigration Act 2009.

ETA data

3. Passport holders of some countries and territories do not have to apply for a visa before they travel to New Zealand, however, they must hold a New Zealand ETA.

4. ETA data is collected by INZ and captures personal information for passport holders from visa waiver countries who apply for and are granted an ETA. A subset of the data held by INZ has been approved for being made available to NZSIS, including the following information:

   i. citizenship;

   ii. passport details;

   iii. name;

   iv. date of birth;

   v. place of birth;

   vi. gender;

   vii. nationality;

   viii. residential address;

   ix. email address;

   x. whether or not the individual has been convicted of an offence; and

   xi. other transaction data related to the ETA being issued.

5. ETA data is 'as supplied' by the applicant and is not validated per se by INZ (except an identity check to inform the ETA issuance). As per the Immigration Act 2009, the ETA

[1] INZ is part of the Ministry of Business, Innovation and Employment.

database is held by the Ministry of Business, Innovation, and Employment ("**MBIE**")[2] and is administered by INZ.

APP data

6. APP data contains personal information for all international air passengers and crew travelling to and departing from New Zealand. The APP dataset captures the following information for New Zealand citizens and permanent residents, as well as foreign nationals:

   i. name;

   ii. date of birth;

   iii. gender;

   iv. nationality;

   v. passport number or certificate of identity number;

   vi. passport or certificate of identity expiry date; and

   vii. the issuer of the person's certificate of identity (if any) if it is not the person's country of nationality.

7. APP data also captures information identifying the craft and its intended movements.

8. As per the Immigration Act 2009, the APP database is held by MBIE [3] and is administered by INZ.

Part 2: NZSIS Responsibilities

9. NZSIS direct access to the APP database and ETA database must comply with the terms of the DAA, as signed by the Minister responsible for Immigration and the Minister responsible for NZSIS.[4]

Using ETA data and APP data

10. In accordance with the terms of the DAA and the legislative requirements of the ISA, NZSIS must ensure that:

    i. any data provided by INZ via direct access is used only for the purposes of NZSIS functions as agreed upon in the DAA; and

[2] Referred to as the "holder agency".
[3] Referred to as the "holder agency".
[4] Before entering into a DAA, both Ministers must be satisfied that direct access to the information is necessary to enable NZSIS to perform any of its functions, there are adequate safeguards to protect the privacy of individuals and the agreement will include appropriate procedures for direct access, use, disclosure, and retention of the information.

ii. ETA data and APP data is used in a way that is necessary and proportionate to NZSIS functions.

Protecting ETA data and APP data

11. In accordance with the terms of the DAA and the legislative requirements of the ISA, NZSIS must ensure there are adequate safeguards in place to protect INZ information. This includes ensuring that there are:

    i. clear procedures for accessing, using, disclosing and retaining INZ information;

    ii. appropriate measures for protecting the privacy of individuals identified by ETA data and APP data; and

    iii. sufficient compliance and audit requirements for the direct access, use, disclosure, and retention of INZ information.

12. For a more detailed description of the ways in which NZSIS will fulfil these responsibilities, see **Part 4: Use of ETA and APP data** and **Part 5: Protecting ETA and APP data**.

NZSIS ownership

13. For a list of Relevant Officers[5] responsible for ensuring NZSIS is compliant with the obligations outlined in the DAA, refer to Appendix 1.

[5] Relevant Officer means NZSIS employees, officers, secondees, and contractors, and GCSB employees, officers, secondees, and contractors required to undertake duties under the DAA on NZSIS's behalf (such as those in the shared Technology and Data Directorate).

Part 3: Scope

In scope

14. This Privacy Impact Assessment (**PIA**) should be read in conjunction with the DAA between the Minister responsible for NZSIS and the Minister responsible for Immigration. This PIA:

    i. identifies the privacy concerns and considerations associated with NZSIS having direct access to ETA data and APP data; and

    ii. outlines the ways in which NZSIS will access, use and protect ETA data and APP data in order to adequately mitigate these privacy concerns.[6]

Out of scope

15. This PIA does not cover any potential access to ETA data and APP data by any other person or agency, except Government Communications Security Bureau (**GCSB**) employees, officers, secondees, and contractors required to undertake duties under the DAA on NZSIS's behalf (such as those in the shared Technology and Data Directorate), or where disclosure is authorised in accordance with section 13 of the Direct Access Agreement.

Releasability

16. This PIA was made available to the offices of the Privacy Commissioner and the Inspector General of Intelligence and Security (**IGIS**) during drafting for their consideration and advice. A copy was also provided to INZ as part of the process to develop the ETA and APP direct access agreement.

17. This PIA details how ETA data and APP data will be handled and used by NZSIS. To protect practices and priorities relating to national security, this unclassified version of the Restricted PIA is published, together with the DAA.

Part 4: Use of ETA data and APP data

ETA data

18. Individuals from visa waiver countries intending to travel to New Zealand must hold an ETA before their scheduled travel to New Zealand. INZ specifies that individuals from visa waiver countries apply at least 72 hours before their scheduled departure for travel to New Zealand.

19. The ETA system:

[6] This covers the entirety of the information management lifecycle (receipt, storage, access, use, retention and disposal) of ETA data and APP data by NZSIS.

i. enables foreign nationals, traveling on a passport from a visa waiver country, to apply for their ETA online ahead of their scheduled travel to New Zealand;[7] and

ii. allows INZ to identify individuals from visa waiver countries intending to travel to New Zealand at least 72 hours before their scheduled boarding time in their country of departure.

20. The ETA is primarily used by INZ as a mechanism to improve border security, by enabling INZ to screen ETA holders before they embark on travel to New Zealand and identify anyone who poses a risk to New Zealand's security.[8]

21. There is significant opportunity for NZSIS to utilise ETA data in the same way, to support our statutory functions of maintaining and enhancing New Zealand's national security.

APP data

22. The APP system enables airlines to check passenger visa and passport details before the passenger boards the aircraft, as well as running checks against INZ border alerts. This allows airlines to identify whether the passenger is noted as a "Board" or "NOT Board" within the INZ system for the purposes of enhancing border security.[9]

23. While APP data is collected primarily for the purposes of maintaining New Zealand's border security, there is significant opportunity for NZSIS to utilise APP data for the purposes of maintaining and enhancing New Zealand's national security.

NZSIS will use ETA data and APP data to fulfil its statutory functions

24. NZSIS will use ETA data and APP data in two ways to fulfil its statutory functions and protect the national security of New Zealand:

a. Automated matching (alerts); and

b. Investigative Analysis.

Automated matching

25. Automated matching of ETA data and APP data against NZSIS holdings is undertaken.

26. A match generates an APP or ETA event, which is then triaged to a Relevant Officer for further assessment.

Investigative Analysis

[7] This includes cruise ship passengers and passengers in transit via Auckland International Airport on the way to/from Australia or to/from another country where their visa waiver also applies.
[8] The ETA is also used as a mechanism for collecting the International Visitor Conservation and Tourism Levy.
[9] Reasons for not being permitted to board include not holding a valid visa to travel to New Zealand.

27. Investigative Analysis refers to user-driven searches of ETA data and APP data to meet general investigative, operational and security requirements.

28. Relevant Officers may undertake specific searches of APP and ETA data to:

    i. complete leads resolutions;

    ii. assess the level of security threat (if any) posed by an individual; and

    iii. identify how to engage with INZ or other agencies regarding a security threat.

29. Investigative Analysis may also be undertaken as part of discovery work, to generate investigative leads (that is, to identify people of security concern that NZSIS is not yet aware of, and should be). This allows NZSIS to identify additional actions the agency should undertake to maintain/protect the national security of New Zealand.

NZSIS will use ETA data and APP data in a way that is necessary and proportionate

30. The data held in the segregated ETA and DAA datasets provides significant intelligence value to NZSIS in terms of its ability to undertake searches that are necessary for the purposes of undertaking NZSIS's specific statutory function(s).[10] The ability for NZSIS to be aware of the travel and travel intentions of individuals of security concern is one of the fundamental capabilities the organisation relies upon in mitigating security threats or ensuring appropriate protective measures are taken.

31. Access to data records such as APP and ETA allows NZSIS to maintain situational awareness without deploying more intrusive capabilities. International travellers are aware that data about their travel is universally employed for security purposes.

32. The use and retention of APP and ETA data is explained in more detail below.

33. The type and circumstances in which the information is collected (personal information and travel details from the traveller themselves), the processes in place for searching the data, and the segregation and security of the datasets ensures unintended impacts are mitigated. Continued access to the full data record is therefore considered proportionate.

Part 5: Protecting ETA data and APP data

Secure data ingestion and storage

34. ETA data and APP data will be transferred from INZ to NZSIS via an approved secure file transfer protocol workflow and is held in a segregated database in NZSIS's security accredited Top Secret network for processing, storage and use.

[10] NZSIS functions include intelligence collection and analysis, protective security services, advice and assistance, cooperation with other public authorities to facilitate their functions and cooperation with other entities to respond to imminent threat.

Access to ETA data and APP data

Access to the Top Secret network

35. Access to the Top Secret network is strictly controlled in accordance with New Zealand security standards for Top Secret networks. Access to the network is restricted to personnel that have been security vetted to the highest level (Top Secret Special).

Access to ETA data and APP data is limited to those with the need to know

36. Not all NZSIS staff have access to ETA data and/or APP data. The entire datasets themselves are maintained in secure, segregated databases. NZSIS use of ETA data and APP data is via automated matching (alerts), with potential matches brought across into the NZSIS main intelligence analysis system for further intelligence development, or through the submission by a Relevant Officer of an approved Investigative Analysis query to return a subset of ETA data and/or APP data for further analysis against other intelligence holdings.

37. Access to ETA data and APP data that has been retrieved and brought into the NZSIS main intelligence analysis system is available to staff working in intelligence and security roles, plus essential enabling services (e.g. legal advisors, information managers, compliance staff, etc.).

38. The NZSIS Legal and Compliance team maintain a record of Relevant Officers (those who have undergone the appropriate training) with such access, and this record is subject to regular review and reporting requirements.

Access auditing

39. Each instance of access to ETA data and APP data held in NZSIS's system (including system administrator access) automatically generates detailed audit log data. Audit log data is available for security and compliance reviews, both by NZSIS and the IGIS.

Disclosure of ETA data and APP data to other parties

40. Selected ETA data and APP data may be provided to other New Zealand government departments or overseas intelligence partners if there is a clear operational rationale to do so.[11] Any information sharing pertaining to ETA data and APP data will be conducted in accordance with the DAA, as well as Ministerial Policy Statements and NZSIS policies.

Retention of ETA data and APP data

41. NZSIS will fulfil its statutory obligations and act in accordance with any Ministerial Policy Statement regarding the retention and disposal of data.

Retaining ETA data and APP data

[11] For example to verify an individual's identity or in support of joint investigative work.

42. NZSIS will retain the full set of 'raw' ETA data and APP data for 25 years from the date it is received (ETA data) and from the date of check-in (APP data). A rolling deletion approach ensures that data is not held beyond this date.

43. The 25-year retention period is an increase from 10 years in the previous DAA. A review of the appropriateness of the retention period concluded that the previous period did not fully account for the attributes of the type of targets of ongoing concern to NZSIS. APP and ETA data held that has not reached 10 years retention and therefore has not been destroyed under the terms of the previous DAA, will have the 25-year retention period applied to it.

44. Any ETA data and APP data that generates an alert will be subject to further processing by NZSIS and will be retained, managed, and stored for as long as it remains relevant, subject to the Public Records Act 2005 and associated disposal authorities. Alerts that are assessed as 'true matches' (i.e. the individual applying for the ETA and/or the individual checking in is the same individual as that in NZSIS holdings) will be retained as part of NZSIS's intelligence knowledge base and used to generate further intelligence or security advice. Alerts that are undetermined or determined to be false matches will be clearly marked as such and retained primarily for the purpose of improving the operation of any automated processing used in NZSIS.

45. When ETA data and APP data is brought across into NZSIS systems for investigative analysis, it may all be deemed to be relevant to an intelligence objective (and retained as a business record of the organisation). Alternatively, it may be subject to further querying to identify information of long-term intelligence value that will be retained. Information which is no longer required is deleted.

Part 6: Privacy risks and mitigations

46. The table below outlines the privacy risks associated with NZSIS's access to ETA data and APP data and the steps that NZSIS will take to mitigate these risks. The residual risk rating assigned to each risk will align with a value in the Risk Management Risk Rating Matrix outlined in Appendix 3.

RISK 1
Insecure transfer or storage of ETA data or APP data, leading to access by an unauthorised external person

Impacts	*Summary of mitigations*
ETA data and APP data captures a large volume of personal and travel information about New Zealand citizens and foreign nationals. Unauthorised access to this information by an external party (a member of the public or a hostile foreign intelligence service hacking into the information) may result in the following impacts: • a major breach of the Privacy Act 2020; • significant negative impact on public trust and confidence in NZSIS and the reputation of NZSIS; • significant negative impact on the relationship between NZSIS and INZ; • possible use by a hostile actor to enhance its own capabilities and/or undermine the national security of New Zealand.	NZSIS takes extensive steps to ensure ETA data and APP data is transferred and stored securely. **Data transfer** • ETA data is ingested into a secure, segregated database within NZSIS systems in batches. APP data is ingested into a secure, segregated database within NZSIS systems in batches. ETA data and APP data is transferred from INZ to NZSIS via an approved secure file transfer protocol workflow. **Data storage + systems access** • all ETA data and APP data retention and access is conducted on NZSIS's Top Secret network. • access to the network is strictly controlled in accordance with New Zealand security standards for Top Secret networks. • access is only granted to Relevant Officers, all of whom have been security vetted to the highest level (Top Secret Special). **Systems Certification and Accreditation (C&A)** • the network is classified at TOP SECRET (the highest level of government network security) and is fully security accredited by GCSB. **Access auditing** • all access by Relevant Officers to ETA data and APP data (including system administrator access and Investigative Analysis searches) is subject to proactive protective monitoring. • regular audits and reviews of access to ETA data and APP data by Relevant Officers are carried out by the NZSIS Compliance team. These reviews are made available to the IGIS.

Residual Risk Rating		
Likelihood: RARE	Impact: CRITICAL	Residual Risk Rating: **MEDIUM**

RISK 2
Unauthorised and/or inappropriate access to ETA data and APP data by Relevant Officers

Impacts	*Summary of mitigations*
ETA data and APP data captures a large volume of personal and travel information about New Zealand citizens and foreign nationals. Unauthorised and/or inappropriate access to ETA data and/or APP data by a Relevant Officer may have a range of impacts, depending on the nature and extent of that access. This could include, but is not limited to: • a moderate breach of the Privacy Act; • moderate impact on public trust and confidence in NZSIS and the reputation of NZSIS; • minor impact on the relationship between NZSIS and INZ.	NZSIS takes extensive steps to ensure ETA and APP information is only accessed by Relevant Officers who are authorised to access the ETA data and/or APP data for appropriate purposes. ***Systems mitigations*** **Systems Certification and Accreditation (C&A)** • NZSIS requires any technical solution to undergo certification and accreditation before it will be approved for wider NZSIS use by intelligence staff. **Access Control Groups (ACGs)** • The datasets are ingested and maintained in secure, segregated databases administered by only a small number of Relevant Officers. • access to ETA data and APP data within the segregated databases by Relevant Officers is only accessible by way of the mechanisms outlined in 8.2.1 and 8.2.2 of the DAA. • access to ETA data and APP data that has been brought into NZSIS main intelligence system is limited using system settings that ensure only Relevant Officers have access to ETA data and/or APP data. • the NZSIS Legal and Compliance team maintain a record of Relevant Officers with access permissions that grant them access to ETA data and APP data that has been retrieved for use. **Systems access auditing** • all access to NZSIS systems is monitored and unusual or suspicious activity is highlighted, including access to ETA data and APP data held in NZSIS's intelligence analysis system (including system administrator access). • regular audits and reviews of access to ETA data and APP data by Relevant Officers are carried out by NZSIS Compliance team. These reviews are made available to the IGIS. ***Operational mitigations*** **Vetting** • all NZSIS employees are vetted to the highest possible level of security clearance (Top Secret Special); the vetting process aims to ensure that NZSIS employees will act with honesty and integrity, including abiding by any NZSIS requirements for accessing, using or sharing ETA data and APP data. **Training** • all Relevant Officers who need to access NZSIS's intelligence analysis system for their role receive full training on the system, including training on their responsibilities in searching for and accessing information appropriately. • the online training module is mandatory for all Relevant Officers who need to access ETA data and/or APP data to fulfil an intelligence function as part of their role. **Managerial oversight**

- NZSIS managers are responsible for ensuring employees are aware of their obligations and only access information that is reasonably required to enable them to carry out their official duties as part of NZSIS's functions.

Compliance and monitoring

- the NZSIS Chief Privacy Officer is responsible for advising the Director-General of Security and the Senior Leadership Team (SLT) on the adequacy of NZSIS systems for dealing with personal information and compliance with the Privacy Act 2020 and steps to be taken to promote robust privacy practices.
- NZSIS Compliance staff oversee the development, implementation and compliance with relevant policies, including information management and access policies.
- NZSIS has a dedicated security team who monitor all access to NZSIS information systems.
- unauthorised and/or inappropriate access to ETA data and APP data will be treated as a security breach; ETA data and APP data security breaches will be investigated, and may lead to disciplinary action.
- section 114 of the Privacy Act 2020 requires mandatory notification to the Privacy Commissioner as soon as practicable after an agency becomes aware that a notifiable privacy breach has occurred.

Strategic mitigations

Policies, Standard Operating Procedures (SOPs) and user agreements

- all Relevant Officers must comply with ETA data and APP data access and usage requirements outlined in NZSIS policy and SOP documentation, as well as the provisions set out in the Direct Access Agreement.
- all Relevant Officers are required to complete an electronic information access agreement declaration, confirming their understanding of acceptable and unacceptable uses of New Zealand Intelligence Community systems and information prior to any system access being granted.
- all Relevant Officers must read and comply with their employment Code of Conduct, which outlines requirements for access to sensitive information.
- failure to comply with NZSIS policies, SOPs, user agreements and/or the NZSIS code of conduct will be investigated and may result in disciplinary action.

Internal work programmes

- NZSIS has an ongoing work programme regarding unauthorised and/or inappropriate access to information that includes reviewing user and system administrator accesses to ensure the appropriate level of restrictions are in place; ongoing review and improvement of security controls relating to access/removal of information from NZSIS systems; and reviewing audit log data requirements relating to system usage.

Residual Risk Rating		
Likelihood: RARE	Impact: MODERATE	Residual Risk Rating: **LOW**

RISK 3
Unauthorised and/or inappropriate sharing of ETA data and/or APP data with a domestic or international agency

Impacts	*Summary of mitigations*
Sharing selected ETA data and APP data with external agencies (both domestic and international) is routine practice for NZSIS. NZSIS shares ETA data and APP data with external agencies in order to meet a range of operational requirements, including: • to verify an individual's identity; • to obtain further details; or • to progress joint national security investigations. Unauthorised and/or inappropriate sharing of ETA data and/or APP data with an external agency may have a range of impacts depending on what information is shared and who it is shared with. This could include, but is not limited to: • a major breach of the Privacy Act; • significant negative impact on public trust and confidence in NZSIS and the reputation of NZSIS; • significant negative impact on the relationship between NZSIS and INZ.	NZSIS takes extensive steps to ensure all information shared with external agencies, including ETA data and APP data obtained via direct access, is shared in a way that is authorised and appropriate. **Training** • Relevant Officers, whose role is to fulfil an intelligence function, must complete mandatory training regarding Information Management and Human Rights. • Relevant Officers must complete the Information Management training module as soon as possible following induction. • Relevant Officers who regularly interact with overseas parties must complete two Human Rights training modules as soon as possible following induction and conduct refresher training; these training modules outline the requirements for Relevant Officers to adhere to New Zealand's human rights obligations. ***Procedural mitigations*** • ETA data and/or APP data may only be provided by NZSIS to other New Zealand Government departments or overseas intelligence partners in accordance with the ISA, MPSs, NZSIS policies and SOPs. • NZSIS Managers are responsible for ensuring that any information released to external agencies (both foreign and domestic) meets NZSIS information sharing requirements. • any unauthorised and/or inappropriate sharing of information with an external agency would be treated as a security breach and prompt an investigation. Security breach investigations may lead to disciplinary action. ***Systems mitigations*** • NZSIS can only share written information with external agencies via secure information sharing mechanisms. • these information sharing mechanisms generate detailed audit log data, which is available for security and compliance auditing, both by NZSIS security officers, the NZSIS Compliance team, and the IGIS. • physical transfer of information off the network for the purposes of sharing the information with an external agency must be appropriately authorised and comply with NZSIS information security standards.
	Residual Risk Rating

	Likelihood: RARE	Impact: MODERATE	Residual Risk Rating: **LOW**

RISK 4 **ETA data and/or APP data is retained for longer than necessary within NZSIS systems**			
Impacts	***Summary of mitigations***		
Retention of ETA data and/or APP data (and therefore personal information) for longer than necessary may constitute a moderate breach of the Privacy Act.	NZSIS takes extensive steps to adequately satisfy implied destruction obligations under the Privacy Act as well as retention obligations under the Public Records Act. In designing the information handling regime for ETA data and APP data, NZSIS has determined 25 years is appropriate to retain the original raw data received from Immigration NZ. All ETA data and APP data that is retrieved by an automated alert or is brought into the NZSIS intelligence analysis system following an analytical query is information that has featured in a legitimate NZSIS function, and is maintained as a business record and retained in accordance with our agreed disposal schedule. Retention of the information for 25 years is required for the purposes for which the information may lawfully be used, and the benefits of retaining the data for 25 years is considered proportionate to the type of information and circumstances in which it was collected, the segregation and security in which it is held, and the specificity and need required to search it. NZSIS has automated the process of securely destroying APP and ETA data from the designated segregated database when its retention period is reached.		
	Residual Risk Rating		
	Likelihood: RARE	Impact: MINIMAL	Residual Risk Rating: **LOW**

Appendix 1: NZSIS Roles and Responsibilities

1. The **Director-General of Security** is responsible for ownership of all NZSIS information assets, with the authority to delegate ownership to the Director Data and Information (DDI).

2. The **Director Data and Information (DDI)** is responsible for:

    i. the management and flow of information, including ETA data and APP data;

    ii. ensuring the risk mitigations outlined in this Privacy Impact Assessment (PIA) are implemented across NZSIS;

    iii. coordinating with the NZSIS Legal and Compliance team to address any issues relating to this PIA; and

    iv. providing leadership and direction for information management in NZSIS, including the management of ETA and APP data.

3. The **NZSIS Chief Privacy Officer** is responsible for:

    i. advising NZSIS Senior Leadership on the adequacy of NZSIS systems for storing, managing and protecting ETA and APP data;

    ii. monitoring compliance with the Privacy Act, in conjunction with the Legal and Compliance team Managers;

    iii. promoting robust privacy practices across NZSIS; and

    iv. overseeing investigations into complaints lodged with the Privacy Commissioner regarding NZSIS access to or use of ETA and/or APP data.

4. The **Manager Ministerial Services and Accountability** is responsible for:

    i. managing and responding to Official Information Act requests and Privacy Act requests on behalf of NZSIS; and

    ii. managing privacy issues in conjunction with other relevant business units.

5. The **Manager Border Assessments** is responsible for:

    i. acting as the operational lead for access to, and use of, ETA data and APP data by NZSIS teams; and

    ii. acting as the primary operational point of contact with INZ to redress ETA and/or APP issues and manage ETA and APP systems/process improvements across agencies.

Appendix 2: Privacy Principles

1. ETA data and APP data collected by INZ contains personal information for all international air passengers and crew traveling to and departing from New Zealand.[12]
2. NZSIS will take all reasonable and necessary steps to minimise the privacy impacts associated with the ingestion and use of ETA data and APP data obtained under the Direct Access Agreement (DAA) in order to:
    i. fulfil our obligations under the DAA;
    ii. fulfil our obligations under the Privacy Act;
    iii. maintain credibility and public confidence in NZSIS's privacy standards.
3. Table 1 provides an assessment of NZSIS's compliance with the 12 privacy principles outlined in the Privacy Act, in relation to the use of ETA data and APP data obtained under the DAA for NZSIS's statutory functions.

Table 1. NZSIS Privacy Principles Assessment

	Privacy Principle as per the Privacy Act	NZSIS assessment against privacy principle	Compliance with Privacy Principle?
1	**Purpose of the collection of personal information** *Collection of personal information by an agency must be lawful and necessary to the function of the agency*	NZSIS has access to ETA data and APP data for the purpose of undertaking its statutory functions. NZSIS access to ETA data and APP data is **lawfully** authorised under the Schedule 2 of the Intelligence and Security Act 2017 (ISA). Information is considered **necessary** where it is required to support the performance of NZSIS's statutory functions: • intelligence collection and analysis; • protective security services, advice, and assistance; • co-operation with other public authorities to facilitate their functions; • co-operation with other entities to respond to imminent threat.	Compliant
2	**Source of personal information** *Get it directly from the people concerned wherever possible.*	If NZSIS were to collect ETA data and APP data directly from the individual, this may: • prejudice the purposes of the collection; and • would not be reasonably practicable in the circumstances. NZSIS is exempt from Information Privacy Principle (IPP) 2 under s28 of the Privacy Act; however, NZSIS access to ETA data and APP data via INZ is lawful as per Schedule 2 of the ISA.	Exempt under s28 of the Privacy Act
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.*	The DAA between INZ and NZSIS is publicly available and makes it clear that NZSIS has access to ETA data and APP data collected by INZ for the purposes specified in the DAA.	Exempt under s28 of the Privacy Act

[12] For ETA data, this includes cruise ship passengers and passengers in transit via Auckland International Airport on the way to/from Australia or to/from another country where their visa waiver also applies.

		While it is public knowledge that NZSIS has **access** to ETA data and APP data, details of exactly when and how NZSIS **uses** ETA data and APP data are not available to the public in order to protect national security practices. For this reason, NZSIS is exempt from IPP3 under s28 of the Privacy Act.	
4	**Manner of collection of personal information** Personal information shall not be collected by an agency (a) by unlawful means; or (b) by means that, in the circumstances of the case (i) are unfair; or (ii) intrude to an unreasonable extent upon the personal affairs of the individual concerned. *Be fair and not overly intrusive in how you collect the information*	IPP4(a): NZSIS access to ETA data and APP data is lawful as per Schedule 2 of the ISA. IPP4(b): NZSIS access to ETA data and APP data is exempt from IPP4(b) under s28 of the Privacy Act.	Compliant with IPP4(a) Exempt from IPP4(b) under s28 of the Privacy Act
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*	All ETA data and APP data is ingested and stored in secure databases on a fully security accredited Top Secret network. NZSIS takes extensive measures to ensure storage and access to ETA data and APP data is secure. Staff are appropriately cleared and trained to utilise the information kept in these databases. Additionally, all log-ins are recorded and subject to compliance reviews.	Compliant
6	**Access to personal information** *People can see their personal information if they want to*	Under the Privacy Act, an individual has the right to seek confirmation from both INZ and NZSIS about whether personal information is held about them. INZ is responsible for the collection of ETA data and APP data from the source, therefore INZ is best placed to handle information requests from individuals regarding their ETA data and/or APP data. Responses to general Privacy Act requests to NZSIS will acknowledge that NZSIS has direct access to databases from other government departments as detailed in the ISA; but we will not search APP data as part of our response to Privacy Act requests of NZSIS.	Compliant
7	**Correction of personal information** *They can correct it if it's wrong, or have a statement of correction attached.*	Under the Privacy Act, an individual has the right to request that their personal information is amended if it is incorrect. INZ is best placed to handle requests from individuals regarding corrections to their ETA data and/or APP data. Any requests to NZSIS regarding corrections to an individual's ETA data and/or APP data will be transferred to INZ.	Compliant
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*	INZ has established procedures with air carriers to ensure the accuracy of APP data (most notably that all personal information must be as shown in the individuals' passport or certificate of identity). NZSIS operational procedures require Relevant Officers to undertake rigorous analysis of the individual's case against intelligence holdings to confirm their identity **before** acting on ETA data and/or APP data. Where an ETA match and/or an APP match is manually assessed to be incorrect, details from the data in the Alert is used to assist in tuning the matching process.	Compliant

9	**Not to keep personal information for longer than necessary** *Get rid of it once you're done with it.*	The full set of 'raw' ETA data and APP data received from INZ will be retained for 25 years to enable the identification of any previous travel / intention to travel that would be of security interest. A review of the retention period was conducted by NZSIS in accordance with the terms of the previous DAA. Retention of the information for 25 years is required for the purposes for which the information may lawfully be used, and the benefits of retaining the data for 25 years is considered proportionate to the type of information and circumstances in which it was collected, the segregation and security in which it is held, and the specificity and need required to search it. Any ETA data or APP data that has featured in an Alert or is brought into the main NZSIS intelligence analysis system following an Investigative Analysis query is maintained as a business record of NZSIS, with disposal arrangements as agreed in the Public Records Act disposal authority.	Compliant
10	**Limits on use of personal information** *Use it for the purpose you collected it for, unless one of the exceptions applies.*	IPP10 states that an intelligence and security agency that holds personal information that was obtained in connection with one purpose may use the information for any other purpose (a secondary purpose) if the agency believes on reasonable grounds that the use of the information for the secondary purpose is necessary to enable the agency to perform any of its functions. In addition, the following exemptions may also be applicable in some circumstances: • (1)(a) directly related to the purpose in connection with which the information was obtained; • (1)(e)(i) to avoid prejudice to the maintenance of the law; and • (1)(f)(i) to prevent or lessen a serious threat to public health or public safety.	Compliant
11	**Limits on disclosure of personal information** *Only disclose it if you've got a good reason, unless one of the exceptions applies*	Under section 10 of the ISA, NZSIS is authorised to provide any intelligence collected and any analysis of that intelligence to the Minister, the Chief Executive of DPMC, and any person or class of persons (whether in New Zealand or overseas) authorised by the Minister to receive the intelligence and any analysis. Under section 11 of the ISA, NZSIS is authorised to, amongst other things, provide protective security service, advice and assistance to any public authority (whether in New Zealand or overseas), and any person or class of persons (whether in New Zealand or overseas) authorised by the Minister. Under s13 of the ISA, NZSIS is authorised to cooperate with certain other New Zealand government departments or overseas intelligence partners. Under section 14 of the ISA, NZSIS is authorised to provide advice and assistance to anyone responding to an imminent threat to the life or safety of any person in New Zealand, or any New Zealand citizen or permanent resident overseas, any person in any area that New Zealand has search and rescue responsibilities for, or any person outside the territorial jurisdiction of any country. Disclosure of personal information (including ETA data and/or APP data when ingested into NZSIS intelligence holdings) for the above purposes by NZSIS will occur in accordance with the exception in IPP11(1)(g), namely where necessary to enable NZSIS to perform any of its functions. Other exceptions that may also be relevant include: • (1)(a) disclosure is one of the purposes (or directly related) for which information was obtained;	Compliant

		• (1)(e) disclosure is necessary to avoid prejudice to the maintenance of the law or for Court proceedings; • (1)(f) disclosure is necessary to prevent or lessen a serious threat to public health or public safety.	
12	**Disclosure of personal information outside New Zealand**	Under s10 of the ISA, NZSIS is authorised to provide any intelligence collected and any analysis of that intelligence to the Minister, the Chief Executive of DPMC, and any person or class of persons (whether in New Zealand or overseas) authorised by the Minister to receive the intelligence and any analysis. Under section 11 of the ISA, NZSIS is authorised to, amongst other things, provide advice and assistance to any public authority (whether in New Zealand or overseas), any person or class of persons (whether in New Zealand or overseas) authorised by the Minister. Protective security services, advice, and assistance includes for the purposes of providing advice and assistance around personnel, information, and physical security, as well as advice around national security risks. Under s13 of the ISA, NZSIS is authorised to cooperate with certain other New Zealand government departments or overseas intelligence partners. Under section 14 of the ISA, NZSIS is authorised to provide advice and assistance to anyone responding to an imminent threat to the life or safety of any person in New Zealand, or any New Zealand citizen or permanent resident overseas, any person in any area that New Zealand has search and rescue responsibilities for, or any person outside the territorial jurisdiction of any country. Any information sharing undertaken by NZSIS is conducted in accordance with the DAA, as well as Ministerial Policy Statements and NZSIS policies. Disclosure of personal information by NZSIS outside New Zealand is for the purposes of IPP11(1)(g). However, should disclosure outside of New Zealand occur in reliance on IPP 11(1)(a), (c), (e), (f), (h), or (i) then IPP 12 would apply.	Compliant
13	**Unique identifiers** *Only assign unique identifiers where permitted.*	NZSIS will not assign unique identifiers to ETA data or APP data.	Compliant

Appendix 3: Risk Management

Table 3: Risk Rating Matrix

The residual risk rating of each APP/ETA privacy risk has been determined using the Risk Management Risk Rating Matrix below.