New Zealand Security Intelligence Service
Te Pā Whakamarumaru

Advance Passenger Processing (APP) Data

Privacy Impact Assessment Report

Owner	Knowledge Manager
Approved By	Chief Privacy Officer
Approval Date	26 October 2022
Review Date	October 2025

Contents

Part 1: Relevant Legislation

1. Under section 125(1) and Schedule 2 of the Intelligence and Security Act (ISA) 2017, 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 (DAA) between NZSIS and Immigration New Zealand (INZ) [1] came into effect on 26 October 2022 after being signed by both parties on 26 October 2022 and enables NZSIS to access Advance Passenger Processing (APP) data collected by INZ under the Immigration Act 2009.

3. APP data is collected by INZ and contains personal information for all international air passengers and crew traveling to and departing from New Zealand. The APP dataset captures the following personal 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.

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

5. As per the Immigration Act 2009, the APP database is held by the Ministry of Business, Innovation, and Employment ("MBIE")[2] and is administered by INZ.

Part 2: NZSIS Responsibilities

6. NZSIS direct access to APP data must comply with the terms of the DAA, as signed by the Minister responsible for Immigration and the Minister responsible for NZSIS.[3]

Using APP data

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

[1] INZ is part of the Ministry of Business, Innovation and Employment (MBIE)
[2] Referred to as the "holder agency".
[3] 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.

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

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

Protecting APP data

8. In accordance with 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. clear measures for protecting the privacy of individuals identified by APP data; and

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

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

NZSIS ownership

10. For a comprehensive list of NZSIS employees responsible for ensuring NZSIS is compliant with the obligations outlined in the DAA, refer to Appendix 1.

Part 3: Scope

In scope

11. This Privacy Impact Assessment (PIA) report should be read in conjunction with the DAA between NZSIS and INZ. This PIA report

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

    ii. outlines the ways in which NZSIS will access, use and protect APP data in order to adequately mitigate these privacy concerns.[4]

Out of scope

12. This PIA does not cover any potential access to APP data by the Government Communications Security Bureau (GCSB) or any other agency.

Part 4: Use of APP data

13. The APP system enables airlines to check passenger visa and passport details before the passenger boards the aircraft, as well run 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 offshore border security.[5]

14. 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 APP data to fulfil its statutory functions

15. NZSIS uses APP data in two ways to fulfil its statutory functions and protect the national security of New Zealand

    i. automated matching; and

    ii. investigative analysis.

Automated matching

16. Automated matching of APP data against NZSIS holdings is undertaken.

17. A match generates an APP check-in event, which is then triaged to a NZSIS officer for further assessment.

Investigative Analysis

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

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

[5] Reasons for not being permitted to board include not holding a valid visa to travel to New Zealand.

19. NZSIS officers undertake manual searches of APP data in order to

    i. complete simple leads resolutions;

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

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

20. Investigative Analysis is also undertaken as part of discovery work, to generate investigative leads. This allows NZSIS to identify additional actions NZSIS should undertake to maintain/protect the national security of New Zealand.

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

21. NZSIS will only use APP data when it is reasonably necessary for the purposes of undertaking our specific statutory function(s).[6]

22. The way in which the NZSIS uses APP data must be proportionate to the activity we are undertaking. The benefit of using the APP data for the purposes of undertaking NZSIS' statutory functions must outweigh the potential intrusion of privacy that may result from the Service acquiring and retaining the dataset.

Part 5: Protecting APP data

Secure data ingestion and storage

23. APP data is ingested to NZSIS systems in regular batches. APP data is transferred from INZ to NZSIS via an approved secure SFTP workflow.

24. Once APP data is received from INZ, it is transferred to NZSIS's fully security accredited Top Secret network for processing, storage and use.

Access to APP data

25. Access to the Top Secret network is strictly controlled in accordance with New Zealand and Five Eyes security standards for Top Secret networks. Access to the network is restricted to staff who have been security vetted to the highest level (Top Secret Special).

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

26. Not all NZSIS staff have access to APP data; the entire dataset is maintained in a segregated database. NZSIS use of APP data is via automated querying (with potential matches brought across into the NZSIS main intelligence analysis system for further intelligence development), or through the submission of an approved investigative analysis query to return a subset of APP data for further analysis against other intelligence holdings. Access to APP data that has been brought into NZSIS systems is

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

limited to staff working in intelligence and security roles, plus essential enabling services (e.g. legal advisors, information managers, compliance staff, etc.)

27. Access to the APP data that has been brought into the main NZSIS intelligence system is not authorised until the employee has successfully completed mandatory Direct Access compliance training, obtained sign off from their Line Manager and confirmation from the NZSIS Compliance and Risk team.

28. The NZSIS Compliance and Risk team maintain a register of NZSIS employees with such access, and the register is subject to annual audit and reporting requirements.

29. For sensitive investigations, retrieved APP data may be stored in a more restrictive manner, limited to only a specific sub-set of staff. These restrictions will be determined on a case-by-case basis.

Access auditing

30. Each instance of access to APP data held in NZSIS's system (including system administrator access) automatically generates detailed audit log data. Audit log data can support security and compliance auditing, both by NZSIS and the Inspector General of Intelligence Services (IGIS).

Disclosure of APP data to other parties

31. Selected 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.[7] Any information sharing pertaining to APP data will be conducted in accordance with the APP DAA, as well as Ministerial Policy Statements and NZSIS policies.

Retention of APP data

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

Retaining APP data

33. NZSIS will retain the full set of 'raw' APP data for ten years from the date of an individual's check-in. A rolling deletion approach ensures that data is not held beyond this date.

34. Any APP data that generates a check-in alert will be subject to further processing by NZSIS and will be retained as a business record in line with NZSIS's agreed Disposal Authority and associated retention schedule. Alerts that are assessed as 'true matches' (i.e. the individual checking in is the same individual as that in NZSIS holdings) will be retained as part of our 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.

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

35. When 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

36. The table below outlines the privacy risks associated with NZSIS's access to APP data and the steps that NZSIS will take to mitigate these risks. The residual risk rating assigned to each risk is assessed using the NZIC Joint Risk Management Framework outlined in Appendix 3.

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

Impacts	*Summary of mitigations*
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 • 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 that APP data could be used by a hostile actor to enhance their own capabilities and/or undermine the national security of New Zealand	NZSIS takes extensive steps to ensure APP data is transferred and stored securely. **Data transfer** • APP data is ingested to NZSIS systems in regular batches. APP data will be transferred from INZ to NZSIS via an approved secure file transfer protocol (SFTP) workflow. **Data storage + systems access** • all 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 and Five Eyes security standards for Top Secret networks. • access is only granted to NZSIS staff (may be secondees or contractors) 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 NZSIS staff to APP data (including system administrator access and investigative analysis searches) is subject to proactive protective monitoring. • Regular audits and reviews of the use of APP data by NZSIS staff 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 APP data by an NZSIS employee

Impacts	*Summary of mitigations*
APP data captures a large volume of personal and travel information about New Zealand citizens and foreign nationals. Unauthorised and/or inappropriate access to APP data by an NZSIS staff member may have a range of impacts, depending on the nature and the extent of 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 APP check-in information is only accessed by authorised NZSIS staff 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** • raw APP data is sequestered within NZSIS in a separate database. The data in it is not directly accessible to intelligence staff. • access to APP data that has been brought into NZSIS main intelligence system is limited using system settings that ensure only staff with a demonstrated need for access, who have been appropriately briefed on their responsibilities in relation to this data and who have signed an acknowledgement of those responsibilities have access to APP data. • the NZSIS Compliance and Risk team manage access to retrieved APP data and maintain a register of those staff that have access to APP data that has been retrieved for use. • the Direct Access Briefing register is subject to annual audit and reporting requirements. **Systems access auditing** • all access to NZIS systems is monitored and unusual or suspicious activity is highlighted, including access to APP data held in NZSIS's intelligence analysis system (including system administrator access). • Regular audits and reviews of the use of APP data by NZSIS staff 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 APP data. **Training** • all NZSIS staff must complete information management training, including training on their responsibilities in searching for and accessing information appropriately. this training also makes NZSIS employees aware of their information management obligations under the Intelligence and Security Act 2017, the Public Records Act, the Privacy Act, the Official Information Act and the Ministerial Policy Statement (MPS) on information management.

- Specific training on identifying Direct Access information is mandatory for all NZSIS staff that need to access intelligence information as part of their role.
- Intelligence Analysts receive additional role-specific training, which includes detailed instruction relating to accessing and using APP data.
- Any staff who access raw APP data receive additional role-specific training, which includes detailed instruction relating to accessing and using APP data.

Managerial oversight

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

Compliance and monitoring

- NZSIS Privacy Officers are responsible for advising the Director of Security and the SLT on the adequacy of NZSIS systems for dealing with personal information and compliance with the Privacy Act and steps to be taken to promote robust privacy practices.
- the NZSIS Compliance team oversees 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 APP data will be treated as a security breach; APP 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 NZSIS employees must comply with APP access and usage requirements outlined in NZSIS policy and SOP documentation, which reflect the requirements of the APP Direct Access Agreement.
- all NZSIS employees must read and sign an Information Technology and Information Systems Agreement for General Users.
- all NZSIS employees must read and comply with the NZSIS Code of Conduct, which outlines requirements for access to sensitive information contained within NZSIS systems.
- 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 APP data with a domestic or international agency

Impacts	*Summary of mitigations*
Sharing APP data with external agencies (both domestic and international) is routine practice for NZSIS. NZSIS share 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 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 APP data obtained via direct access, is shared in a way that is authorised and appropriate. ***Operational mitigations*** **Training** • NZSIS staff employees must complete mandatory training regarding Information Management and Human Rights. • NZSIS employees must complete the Information Management training module as soon as possible following induction. • NZSIS employees who regularly interact with overseas parties with must complete Human Rights risk management training following induction and must refresh their training on an annual basis; these training modules outline the human rights risk management policy which applies to the activities of NZSIS, and details how this policy is applied when data is shared with international agencies. ***Procedural mitigations*** • APP data may only be provided by NZSIS to other New Zealand government departments or overseas intelligence partners in accordance with the Intelligence and Security Act 2017 (ISA), 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 information with external agencies via secure information sharing mechanisms. • all information sharing mechanisms generate detailed audit log data, which is available for security and compliance auditing. • 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 **APP data is retained for longer than necessary within NZSIS systems**			
Impacts	***Summary of mitigations***		
Retention of APP data (and therefore personal information) for longer than necessary would be contrary to IPP9 and 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 APP, NZSIS has determined a reasonable period of time (10 years) to retain the original raw check in data received from Immigration NZ. All 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 in accordance with our agreed disposal schedule (DA692).		
	Residual Risk Rating		
	Likelihood: UNLIKELY	Impact: MINOR	Residual Risk Rating: **LOW**

Appendix 1: NZSIS Roles and Responsibilities

1. The **Director of Security** is responsible for ownership of all NZSIS information assets, with the authority to delegate ownership to the Knowledge Manager.

2. The **Knowledge Manager** is responsible for:

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

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

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

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

    ii. monitoring compliance with the Privacy Act, in conjunction with the Compliance and Risk team Manager;

    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 APP data.

4. The **Manager Strategy and Accountability** is responsible for:

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

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

5. The **Security Assessments Delivery Manager is responsible for:**

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

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

Appendix 2: Privacy Principles

6. APP data collected by INZ contains personal information for all international air passengers and crew traveling to and departing from New Zealand.
7. NZSIS will take all reasonable and necessary steps to minimise the privacy impacts associated with the ingestion and use of 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' privacy standards.
8. Table 1 provides an assessment of NZSIS' compliance with the 13 privacy principles outlined in the Privacy Act 2020, in relation to the use of APP data obtained under the DAA for NZSIS' 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 APP data for the purpose of undertaking its statutory functions. NZSIS access to APP data is **lawfully** authorised under the Schedule 2 of the Intelligence and Security Act (ISA) 2017. Information is considered **necessary** where it is required to support the performance of NZSIS' 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 APP data from the individual, this may • be prejudicial to the maintenance of the law; • prejudice the purposes of the collection; and • would not be reasonable practicable in the circumstances NZSIS is exempt from PP2 under s28 of the Privacy Act; however NZSIS access to 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 publically available and makes it clear that NZSIS has access to APP data collected by INZ. While it is public knowledge that NZSIS have **access** to APP data, details of exactly how NZSIS **uses** APP data are not available to the public in order to protect national security practices. For this reason, NZSIS is exempt from PP3 under s28 of the Privacy Act.	Exempt under s28 of the Privacy Act
4	**Manner of collection of personal information**	PP4(a): NZSIS access to APP data is lawful as per Schedule 2 of the ISA	Compliant with PP4(a)

	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*	PP4(b): NZSIS access to APP data is exempt from PP4(b) under s28 of the Privacy Act	Exempt from PP4(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 APP data is ingested and stored on a fully security accredited Top Secret network. NZSIS take extensive measures to ensure storage and access to APP data is secure.	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 are responsible for the collection of APP data from the source. As the "holder agency", INZ are best place to handle information requests from individuals regarding their 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 Intelligence and Security Act; 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. As the "holder agency", INZ are best place to handle requests from individuals regarding corrections to their APP data. Any requests to NZSIS regarding corrections to an individual's 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 have 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 of certificate of identity). NZSIS operational procedures require employees to undertake rigorous analysis of the individual's case against intelligence holdings to confirm their identity **before** acting on APP data. Where 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' APP data received from INZ will be retained for ten years from the date of check-in, to enable the identification of any previous travel that would be of security interest. Any APP information 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 disposal authority DA692.	Compliant

10	**Limits on use of personal information** *Use it for the purpose you collected it for, unless one of the exceptions applies.*	PP10 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. NZSIS uses APP data for near real-time and retrospective matching of individuals against NZSIS holdings, in line with NZSIS' statutory functions. The use of APP data for investigative analysis is necessary to enable NZSIS to perform its statutory functions. This use is therefore permitted under exemptions under IPP10, including (c)(i) to avoid prejudice to the maintenance of the law; (d) public health or public safety; (e) directly related to the purpose in connection with which the information was obtained.	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 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. This 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 other New Zealand government departments 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 comes within the following exemptions to IPP11: (a) disclosure is one of the purposes (or directly related) for which information was obtained; (e) non-compliance is necessary to avoid prejudice to the maintenance of the law or for Court proceedings; (f) necessary to prevent or lessen a serious threat. (g) that the disclosure of the information is necessary to enable an intelligence and security agency to perform any of its functions.	Compliant
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. This 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 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(g). However should sharing disclosure outside of New Zealand occur in reliance on IPP 11(a), (c), (e), (f), (h), or (i) then IPP 12 would apply. (g) that the disclosure of the information is necessary to enable an intelligence and security agency to perform any of its functions.	
13	**Unique identifiers** *Take care when using unique identifiers*	Information drawn from APP and transferred into NZSIS's main intelligence analysis system will be identifiable as personal information; no unique identifiers will be generated except those required by the intelligence analysis system to function as a database.	Compliant