



DIRECT ACCESS AGREEMENT

BETWEEN

**THE MINISTER RESPONSIBLE FOR THE NEW ZEALAND SECURITY
INTELLIGENCE SERVICE (NZSIS)**

AND

THE MINISTER OF IMMIGRATION

1. Parties

- 1.1. This direct access agreement ("DAA") is between the Minister Responsible for the New Zealand Security Intelligence Service ("NZSIS") and the Minister of Immigration (together, "the Parties").
- 1.2. This DAA comes into force upon signature by both parties.

2. Background and Purpose

- 2.1. The Intelligence and Security Act 2017 ("ISA") enables an intelligence and security agency to have direct access to certain specified information contained in certain public sector databases.
- 2.2. The purpose of this agreement is to enable access by NZSIS (as an intelligence and security agency) to information collected by the Ministry of Business, Innovation and Employment ("MBIE") in connection with the performance or exercise of a function, duty, or power under the Immigration Act 2009. The agreement covers access to the Advance Passenger Processing ("APP") and the Electronic Travel Authority ("ETA") databases administered by Immigration New Zealand ("INZ").
- 2.3. The APP database contains travel document information of passengers and crew travelling to and from New Zealand, together with craft identification and movement information. The ETA database contains information submitted by foreign nationals from prescribed visa-waiver countries and territories seeking permission to travel to or transit through New Zealand without being required to hold a valid visa.¹
- 2.4. This DAA replaces the previous DAA concluded in March 2017.

3. Definitions

- 3.1. Terms relevant to this agreement are defined as follows:
 - 3.1.1. **Direct access**, in relation to a database, means to do either or both of the following (whether remotely or otherwise):
 - 3.1.1.1. Search the database;
 - 3.1.1.2. Copy any information stored on the database (including by previewing, cloning, or other forensic methods).
 - 3.1.2. **NZSIS Staff** means NZSIS employees, officers, secondees, and integrated contractors.

¹ A person who is not a New Zealand citizen or permanent resident must hold a valid visa to travel to, enter and remain in New Zealand. Pursuant to s 69 of the Immigration Act 2009, regulations may be made to waive the requirement to hold a visa permitting travel to New Zealand in relation to any class of persons. A regulation has been passed granting such an exemption to individuals from listed nationalities, known as persons from visa-waiver countries. At the date of this DAA there were more than 60 prescribed visa-waiver countries and territories.



- 3.1.3. **APP Information** means all information in the APP database collected, generated, or stored for or by MBIE including:
- 3.1.3.1. Information about inbound and outbound passengers collected from carriers under s 96 of the Immigration Act 2009 (specified in the 'Immigration (Carriers' Information Obligations) Regulations 2010');
 - 3.1.3.2. Decisions about inbound passengers made by the chief executive of MBIE under s 97 of the Immigration Act 2009;
 - 3.1.3.3. Decisions about outbound passengers made by the chief executive of MBIE under s 97A of the Immigration Act 2009; and
 - 3.1.3.4. Incidental transactional information, for example date/time stamps or internal reference numbers, generated by the APP system.
- 3.1.4. **ETA information** means a subset of the information in the Electronic Travel Authority database collected, generated, or stored for or by MBIE in relation to a person who is required to hold an Electronic Travel Authority as a condition of being granted a visa waiver, namely:
- 3.1.4.1. Passport details (including personal and non-personal information);
 - 3.1.4.2. Applicant's contact details;
 - 3.1.4.3. Entry information;
 - 3.1.4.4. Prior criminal convictions (yes/no);
 - 3.1.4.5. eTA type and expiry date;
 - 3.1.4.6. eTA transactional information.
- 3.1.5. **International security standards for intelligence and security agencies** refers to the US Committee for National Security Systems Instruction 1253.
- 3.2 All of the other definitions in this agreement (including but not limited to the definitions of **database** and **information**) have the meaning as described in the ISA unless otherwise noted.

4. Databases to be accessed

- 4.1. The databases to be accessed by NZSIS are the APP database and the ETA database.
- 4.2. The APP database stores, transfers and processes information collected and generated by and for MBIE under ss 96, 97, and 97A of the Immigration Act 2009. Such APP information is used by MBIE to decide whether a person may board a craft travelling to or from New Zealand.
- 4.3. A carrier must provide certain APP information to MBIE as prescribed in the Immigration (Carriers' Information Obligations) Regulations 2010. It consists of travel document information identifying the individual passenger or crew member (e.g. name, passport number), and other information identifying the craft and its intended movements (e.g. the expected place of arrival).

- 4.4. Carriers provide the APP information when a person checks in for an international service. MBIE checks APP information against border agency alerts and records of lost and stolen travel documents. It also confirms whether any visas are valid. It then directs the carrier to either allow or refuse to allow the person to board the craft. Some persons must always be allowed to board a craft (e.g. a person travelling to New Zealand on a New Zealand passport).
- 4.5. The second database to be accessed by NZSIS is the ETA database. The ETA database stores and processes information submitted by foreign nationals from prescribed visa-waiver countries as a prerequisite to obtaining a waiver from the requirement to hold a visa permitting travel to New Zealand. The information submitted as part of the ETA process includes details of a person's identity, travel document, and travel plans.

5. Particular information that may be accessed

- 5.1. NZSIS may access APP information.
- 5.2. NZSIS may access ETA information.
- 5.3. For the avoidance of doubt, neither the APP nor ETA database contain information about claims for, or recognition as, a refugee or protected person in New Zealand.

6. Particular purpose or purposes for which the information may be accessed

- 6.1 APP and ETA information will be accessed by NZSIS for the following purposes:
 - 6.1.1. Screening to identify when individuals assessed to be of security concern or intelligence interest submit a request for an Electronic Travel Authority and/or check in for international travel; and
 - 6.1.2. Conducting intelligence analysis and searches, in response to other information held by NZSIS, in support of the statutory functions specified in section 7 of this agreement. Such analysis of APP and ETA information will, in many cases, enable NZSIS to develop intelligence leads rapidly without requiring the use of more intrusive investigatory measures.
- 6.3 For the avoidance of doubt, NZSIS is not a border security or enforcement agency, however it has a function to provide advice about national security risks and to collect, analyse and provide intelligence in accordance with New Zealand Government priorities.

7 Particular function, duty, or power being, or to be, performed or exercised by NZSIS for which the information is required

- 7.1 NZSIS will access APP and ETA information to support the following statutory functions, as specified in the ISA:
 - 7.1.1 Intelligence collection and analysis; and
 - 7.1.2 Protective security services, advice and assistance. The use of APP and ETA information in this regard by NZSIS includes but is not limited to providing security

advice to INZ in support of immigration and border security decision-making processes.

- 7.2 Additional information on how APP and ETA information will be used to support these functions is outlined in the associated Privacy Impact Assessments (“PIAs”).

8 Mechanism by which information is to be accessed

- 8.1 A copy of all APP and ETA information received by MBIE will be provided electronically to NZSIS in a timely manner. This copy will be held and maintained on NZSIS’s fully security accredited Top Secret network. This copy will be held separately from NZSIS’ intelligence holdings, in a segregated database and is held solely to enable NZSIS’ direct access to APP and ETA information under this agreement.

- 8.2 APP and ETA information will only be accessible by NZSIS Staff by way of:

8.2.1 Alerts, made accessible within NZSIS’s intelligence analysis system, generated when individuals assessed to be of security concern or intelligence interest submit a request for an ETA or check in for international travel; and

8.2.2 Specific search mechanisms for the analysis of APP and ETA information in support of the statutory functions specified in section 7 of this agreement.

- 8.3 Some alerts created from APP and ETA information may generate a further high-level automatic message that will be received by GCSB staff to enable full time coverage of border intelligence in circumstances when NZSIS staff may be unavailable. This automatic message will provide non-personal information to the GCSB staff indicating a potential alert has been received in NZSIS’s system. This will enable the GCSB staff to contact NZSIS staff to make them aware of a potential security concern or intelligence interest.

9 Positions of persons who may access the information

- 9.1 Access to APP and ETA information will be limited to people working for NZSIS on the functions specified in section 7 of this agreement, where access is required to carry out that function (plus enabling staff in technology, information management or compliance roles). All NZSIS Staff granted access to APP and ETA information must first complete training in their legal and policy obligations with regards to accessing the databases, and the use and storage of information accessed.

10 Records to be kept in relation to each occasion a database is accessed

- 10.1 Access to any APP or ETA information held electronically within NZSIS systems will generate detailed audit log data. This data can be used to support security and compliance reviews, including by the Inspector-General of Intelligence and Security or by a suitable cleared employee of MBIE. NZSIS will regularly conduct an audit of its direct access to APP and ETA information to provide assurance that it is accessing this information in accordance with this DAA.

11 Safeguards to be applied for protecting particular information

11.1 Detailed privacy and security safeguards by which APP and ETA information will be protected by NZSIS are set out in the PIAs. They include:

11.2 General Safeguards:

11.2.1 All NZSIS staff are security vetted to the highest level.

11.2.2 All NZSIS staff receive training on the Privacy and Official Information Acts.

11.2.3 All NZSIS staff are subject to the NZSIS Code of Conduct.

11.2.4 All NZSIS staff are required to sign an information access agreement, outlining acceptable and unacceptable uses of NZSIS systems and information, prior to any system access being granted.

11.2.5 All access to and use of NZSIS electronic systems will be logged and subject to security and compliance auditing (both routine and ad hoc) to ensure that access to information is authorised and appropriate in accordance with legislative requirements, NZSIS policies, and the role of the individual NZSIS Staff member.

11.3 Access to APP and ETA information:

11.3.1 APP and ETA information will only be stored on and accessed via a secure accredited network, with all user accounts, access rights, and security authorisations proactively managed and controlled in line with international security standards for intelligence and security agencies;

11.3.2 Access to APP and ETA information will only be possible via the two controlled mechanisms specified in section 8 of this agreement, both of which will generate detailed audit log data;

11.3.3 Initial and ongoing access to APP/ETA information is subject to staff maintaining their annual compliance certification – which includes specific training on appropriate use of information obtain by NZSIS through direct access arrangements with other government departments;

11.3.4 Access to the APP and ETA search mechanisms by NZSIS Staff will be subject to line manager approval that the requester has a legitimate requirement to search and analyse APP/ETA information. Business records (including the NZSIS Staff member conducting the search) will be maintained for all searches of APP/ETA data describing:

- a. Which of NZSIS' statutory functions the search is being done in support of;
- b. Which investigation, operation, project or security clearance case it relates to; and
- c. The reason for the search; and
- d. Identifying details of the NZSIS Staff member conducting the search.

11.3.5 The search mechanisms and associated policies and procedures will, as far as is practicable, ensure that all searches are as narrow and specific as possible.



11.3.6 By default, results provided within the search mechanism will exclude APP and ETA information relating to juveniles (individuals aged 16 or younger on the date of the search). Should NZSIS Staff require information relating to juveniles to be returned in order to carry out a function specified in section 7 of this agreement, this will require prior written approval from an appropriate NZSIS manager.

11.3.7 Initial results of a search of APP/ETA information will be examined by the requester. Only information required for one of the statutory functions described in section 7 of this agreement will be maintained as an intelligence record in the main NZSIS intelligence analysis system. Any information generated by the requester's search deemed to be irrelevant will be destroyed as soon as practicable.

11.3.8 All APP and ETA information brought into the NZSIS intelligence analysis system will be labelled in such a way as to indicate the source so that information obtained via this DAA is identifiable as such to NZSIS.

12 Requirements relating to storage, retention, and disposal of information obtained from the database

12.1 All information accessed from the APP and ETA databases will be handled and stored in accordance with the appropriate security endorsements, caveats, and protective markings and in accordance with the New Zealand Government Protective Security Requirements.

12.2 All APP and ETA information provided by MBIE will be retained by NZSIS for a default period of ten years. A review of the appropriateness of this ten year retention period is to be conducted by NZSIS to inform the next Ministerial review required under clause 19.1.

12.3 Any APP or ETA information that is brought into the database of NZSIS's intelligence analysis system and determined to be relevant to the statutory functions specified in section 7 of this agreement will be retained and managed as public records of NZSIS activities, in accordance with the Public Records Act 2005 and be subject to the usual considerations by NZSIS when any Official Information Act or Privacy Act requests are received.

12.4 Disposal of APP and ETA information will be conducted in accordance with the Public Records Act 2005 and any retention and disposal schedule which governs this action.

13 Circumstances in which the information may be disclosed to another agency (whether in New Zealand or overseas), and how that disclosure may be made

13.1 The ISA provides that NZSIS may share intelligence (and any analysis of that intelligence) with the Minister Responsible for the NZSIS, the Chief Executive of the Department of the Prime Minister and Cabinet and any person or class of persons, whether in New Zealand or overseas, authorised by the Minister Responsible for the NZSIS to receive that intelligence (or analysis). The ISA imposes an additional requirement in relation to the provision of intelligence to any overseas person or class of persons, being that the Minister Responsible for the NZSIS must be satisfied that, in providing the intelligence, NZSIS will be acting in accordance with New Zealand law and all human rights obligations recognised by New Zealand law.

- 13.2 The Minister Responsible for the NZSIS has given Ministerial Authorisations to NZSIS to share intelligence, however those Authorisations are classified. For the purposes of the DAA, it is sufficient to note that the Ministerial Authorisations authorise NZSIS to provide intelligence, and any analysis of that intelligence, to:
- 13.2.1 any New Zealand Government agency including Parliament, the State Sector, Crown Entities, State Owned Enterprises, local government, and other specified government agencies and associated entities;
 - 13.2.2 a number of specified overseas public authorities (including agencies from Australia, Canada, the United Kingdom and the United States of America); and
 - 13.2.3 other specified countries or authorised persons in specified circumstances.
- 13.3 In accordance with the ISA, NZSIS will only disclose APP or ETA information where doing so:
- 13.3.1 will contribute to one of NZSIS's statutory objectives (e. g. contribute to the protection of national security);
 - 13.3.2 falls within one of NZSIS's statutory functions, duties or powers;
 - 13.3.3 is to a person or class of persons (whether in New Zealand or overseas) authorised by the Minister Responsible for NZSIS to receive intelligence and any analysis of that intelligence; and
 - 13.3.4 would not lead to a human rights breach.
- 13.4 Disclosures of APP or ETA information will be made in accordance with the New Zealand Government's Protective Security Requirements and international security standards for intelligence and security agencies, and may be made verbally, electronically or in person.
- 13.5 In addition to the above, when sharing intelligence with external parties NZSIS gives consideration to overarching principles as outlined in internal policy, including the need to consider whether the interaction aligns with NZSIS objectives and New Zealand Government Priorities; the necessity and proportionality of sharing personal information; human rights obligations; and whether the sharing is otherwise restricted or prohibited in any way.

14 Relationship with other legislation

- 14.1 Nothing in this agreement affects NZSIS's ability to request information or MBIE's ability to disclose information under other provisions in the ISA or where the request or disclosure is authorised or required under any enactment, including as permitted by the information privacy principles, however access to APP and ETA information via this DAA is to be preferred unless it is necessary to request the information via other means.

15 Apportionment of costs

- 15.1 All costs associated with processing APP and ETA information within MBIE-owned or controlled systems to enable it to be provided to the NZSIS in a timely manner will be the sole responsibility of MBIE.
- 15.2 All costs associated with the delivery of APP and ETA information to NZSIS following its extraction from MBIE systems, as well as the subsequent processing, storage, access and disposal within NZSIS systems, will be the sole responsibility of NZSIS.



16 Publication of this agreement

- 16.1 This DAA will be published on the MBIE and NZSIS websites.
- 16.2 The associated PIAs will be published, but some information within them remains classified and may be withheld as authorised by section 131(2)(b) of the ISA and in accordance with the Official Information Act 1982.
- 16.3 Before entering into this DAA the Parties consulted with and invited comments from the IGIS and the Privacy Commissioner, and had regard to those comments.

17 Public's right of access

- 17.1 Nothing in this DAA affects an individual's right to make an information privacy request in accordance with the Privacy Act 2020.
- 17.2 Nothing in this DAA affects the ability to make a complaint to the Inspector-General of Intelligence and Security in accordance with section 171 of the ISA.

18 Dispute resolution

- 18.1 In the event of dispute the parties will consult with a view to resolving any issues as soon as practicable.

19 Review of this agreement

- 19.1 This DAA must be reviewed by the Ministers that have entered into this agreement every three years. Ministers are able to review this DAA without the requirement to wait for three years.

Signed



Hon Andrew Little

**Minister Responsible for the New Zealand
Security and Intelligence Service**

Date Signed: 15/8/22



Hon Michael Wood

Minister of Immigration

Date Signed: 26/10/2022