



**DIRECT ACCESS AGREEMENT TO  
ADVANCE PASSENGER PROCESSING (APP) DATABASE  
BETWEEN  
THE MINISTER IN CHARGE OF THE NEW ZEALAND SECURITY INTELLIGENCE  
SERVICE (NZSIS)  
AND  
THE MINISTER OF IMMIGRATION**

## UNCLASSIFIED

### 1. Parties

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

### 2. Background and Purpose

- 2.1. The Intelligence and Security Act 2017 ("ISA") enables an intelligence and security agency to directly access certain public sector databases.
- 2.2. The purpose of this agreement is to enable access by NZSIS (as an intelligence and security agency) to the Advance Passenger Processing ("APP") database held by the Ministry of Business, Innovation, and Employment ("MBIE") pursuant to the Immigration Act 2009 (as the "holder agency").
- 2.3. Immigration New Zealand ("INZ"), a business group within MBIE, administers the Immigration Act 2009.

### 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):
    - 3.1.1.1.1. Search the database;
    - 3.1.1.1.2. Copy any information stored on the database (including by previewing, cloning, or other forensic methods).
- 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. Database to be accessed

- 4.1. The database to be accessed by NZSIS is the APP database. 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.
- 4.2. A carrier must provide certain APP information to MBIE. That information is prescribed in the Immigration (Carriers' Information Obligations) Regulations 2010. It consists of travel document information identifying the individual passenger or crew

UNCLASSIFIED

## UNCLASSIFIED

member (e.g. a passport number), and other information identifying the craft and its intended movements (e.g. the expected place of arrival).

- 4.3. 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).
- 4.4. An APP system was first implemented for inbound carriers in 2003. It allows MBIE and carriers to manage risk before a person boards a craft.

### **5. Particular information that may be accessed**

- 5.1. NZSIS may access all information in the APP database collected, generated, or stored for or by MBIE ("APP information") including:
  - 5.1.1. 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');
  - 5.1.2. Decisions about inbound passengers made by the chief executive of MBIE under s 97 of the Immigration Act 2009;
  - 5.1.3. Decisions about outbound passengers made by the chief executive of MBIE under s 97A of the Immigration Act 2009; and
  - 5.1.4. Incidental transactional information, for example date/time stamps or internal reference numbers, generated by the APP system.
- 5.2. For the avoidance of doubt, the APP database does not 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 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 check in for an international flight; 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 information will, in many cases, enable NZSIS to develop intelligence leads rapidly without requiring the use of more intrusive investigatory measures.

UNCLASSIFIED





**UNCLASSIFIED**

- 6.3 For the avoidance of doubt, in particular in relation to screening when individuals check in for an international flight, NZSIS is not a border security or enforcement agency.

**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 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 information in this regard by NZSIS includes but is not limited to: (a) providing security advice to INZ in support of immigration and border security decision-making processes; and (b) security clearance assessments.

- 7.2 Additional information on how APP information will be used to support these functions is outlined in the associated Privacy Impact Assessment ("PIA").

**8 Mechanism by which information is to be accessed**

- 8.1 A copy of all APP information received by MBIE will be provided electronically to NZSIS as it is received. This copy will be held and maintained on NZSIS's fully security accredited Top Secret network.

- 8.2 APP information will only be accessible by NZSIS employees 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 check in for an international flight; and

8.2.2 A specific search mechanism for the analysis of APP information. Access to this APP search mechanism will be strictly limited, as specified in section 11 of this agreement. Search results will be triaged, before APP information assessed as being relevant to the statutory functions specified in section 7 of this agreement are brought into the database of NZSIS's intelligence analysis system.

- 8.3 Where APP information is brought into and accessible via NZSIS's intelligence analysis system, it will only be retained if it is determined to be relevant.

**9 Positions of persons who may access the information**

- 9.1 Access to APP information will be limited to those NZSIS employees working directly on the functions specified in section 7 of this agreement, where access is required to carry out that function. All NZSIS employees granted access to APP must first complete

**UNCLASSIFIED**



## UNCLASSIFIED

training in their legal and policy obligations with regards to accessing APP, and the use and storage of information accessed through APP.

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

- 10.1 Access to any APP information held electronically within NZSIS systems will generate detailed audit log data. This data will be made available for security and compliance reviews, including by the Inspector-General of Intelligence and Security, and a suitably cleared employee of the Chief Executive of MBIE as per any joint audit agreements entered into between NZSIS and MBIE.

### **11 Safeguards to be applied for protecting particular information**

- 11.1 Detailed safeguards by which APP information will be protected by NZSIS are set out in the PIA. The security and privacy safeguards to be applied include:

11.1.1 Access to APP information will be strictly controlled in accordance with agreed international security standards for intelligence and security agencies;

11.1.2 APP information will only be stored on and accessed via secure networks and systems, with all user accounts, access rights, and security authorisations proactively managed and controlled in line with international security standards for intelligence and security agencies;

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

11.1.4 Access to the APP search mechanism will only be available to NZSIS employees in a relevant role, and will be subject to written confirmation from each NZSIS employee's line manager that they have a legitimate requirement to search and analyse APP information. Access to the APP search mechanism will also be dependant on the NZSIS employee attending and passing an assessed training course specifically covering their legal and policy obligations in relation to APP information. All searches done on APP information in the search mechanism will require the NZSIS employee to identify:

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

11.1.5 This three-part justification, together with the identity of the employee who conducted the search, will be recorded on all APP information that is brought into NZSIS's intelligence analysis system for analysis.

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

UNCLASSIFIED

**UNCLASSIFIED**

- 11.1.7 By default, results provided within the search mechanism will exclude APP information relating to juveniles (individuals aged 16 or younger on the date of the search). Should an NZSIS employee require APP 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.
- 11.1.8 To reduce the potential privacy impact of searches, the amount of APP information able to be brought into NZSIS's intelligence analysis system at any one time will be limited to a specified number of search results. The APP information brought into the system will only be available to NZSIS employees in a relevant role.
- 11.1.9 All NZSIS employees are security vetted to the highest level.
- 11.1.10 All NZSIS employees receive training on the Privacy and Official Information Acts.
- 11.1.11 All NZSIS employees are subject to the NZSIS Code of Conduct.
- 11.1.12 All NZSIS employees 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.
- 11.1.13 All access to and use of NZSIS electronic systems, including access to the APP information, will be logged and subject to security and compliance auditing to ensure that access to information is authorised and appropriate in accordance with legislative requirements, NZSIS policies, and the individual employee's role.

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

- 12.1 All information accessed from the APP database 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 information provided by MBIE will be retained by NZSIS for a default period of ten years.
- 12.3 A review of the suitability of this retention period will be conducted 12 months after the commencement of this DAA, by the parties.
- 12.4 Any APP 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, with a default retention period of 25 years.

**UNCLASSIFIED**



UNCLASSIFIED

12.5 Disposal of APP information will be conducted in accordance with the Public Records Act 2005.

**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 Intelligence and Security Act provides in cl 13(1)(b)(iii) that the Minister in Charge of the NZSIS may authorise the provision of intelligence and any analysis of that intelligence to any person or class of persons, whether in New Zealand or overseas. The Act imposes an additional requirement in relation to the provision of intelligence to any overseas person or class of persons, being that the Minister 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 As the relevant provisions do not come into effect until six months after the date of Royal assent, it is necessary to provide the following transitional measures, which will be superseded by the terms of any Ministerial cl 13 authorisation and the relevant Ministerial Policy Statement. NZSIS will advise MBIE of any changes in obligations with regards to disclosure of information arising from any cl 13 authorisation and/or Ministerial Policy Statement.

13.3 In relation to overseas persons, NZSIS may provide APP information and any analysis of that information (together "APP-Related Intelligence" or "ARI") to intelligence or security agencies from Australia, Canada, the United Kingdom, and the United States of America. In the event the Director of Security determines it is in the interests of security to provide ARI to another overseas person or class of persons, the Director of Security will seek express approval from the Minister in Charge of the NZSIS. The Minister will consider whether the ARI should be provided, having regard to:

- a. the nature and scope of the ARI NZSIS proposes to provide;
- b. the nature of the agency to which NZSIS proposes to provide the ARI; and
- c. whether provision of the ARI would be in accordance with New Zealand law and all human rights obligations recognised by New Zealand law.

13.4 In relation to non-overseas persons, NZSIS may provide ARI to New Zealand Government entities. In the event the Director of Security determines it is in the interests of security to provide ARI to any other non-overseas person or class of persons, the Director of Security will seek express approval from the Minister in Charge of NZSIS. The Minister will consider whether the ARI should be provided, having regard to:

- a. the nature and scope of the ARI NZSIS proposes to provide;
- b. the nature of the agency to which NZSIS proposes to provide the ARI; and

UNCLASSIFIED





**UNCLASSIFIED**

- c. whether provision of the ARI would be in accordance with New Zealand law and all human rights obligations recognised by New Zealand law.
- 13.5 In relation to disclosure of ARI to both overseas and non-overseas entities outside the approved classes outlined above (intelligence or security agencies from Australia, Canada, the United Kingdom, and the United States of America, and New Zealand Government entities), the Minister may impose any conditions or restrictions as he or she considers necessary.
- 13.6 The decision to disclose ARI to any member/s of these authorised classes of non-overseas persons may be made by any NZSIS employee where this is required for carrying out NZSIS's functions. Records of the decision and reasons for the decision will be documented as per NZSIS's record keeping policies.
- 13.7 If the Director of Security reasonably believes:
  - 13.7.1 that it is necessary to share APP or ARI outside of the classes approved by the Minister in order to provide advice and assistance to a person or agency to respond to an imminent threat to the life or safety of an individual or group of individuals; and
  - 13.7.2 it is not possible to obtain the prior approval of the Minister due to the urgent nature of the imminent threat;
  - 13.7.3 the Director of Security may authorise the sharing of ARI to the agency or person concerned. The Director of Security must as soon as possible then advise the Minister.
- 13.8 For the purposes of this agreement, the ARI that is authorised to be shared may relate to one or more identifiable individuals or categories of individuals.

#### **14 Relationship with other legislation**

- 14.1 Nothing in this agreement affects NZSIS's ability to request information under other provisions in the ISA or any other legislation.

#### **15 Apportionment of costs**

- 15.1 All costs associated with processing APP 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 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.

**UNCLASSIFIED**

**UNCLASSIFIED**

16.2 The associated PIA contains sensitive technical and operational information, will not be published, and may be withheld in accordance with the Official Information Act 1982. The PIA was developed in full consultation with MBIE, the Office of the Privacy Commissioner, and the Office of the Inspector-General of Intelligence and Security.

**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 1993.

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 134 of the ISA.

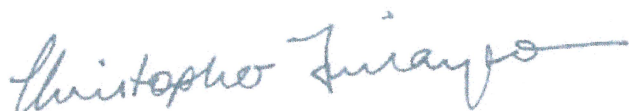
**18 Dispute resolution**

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**

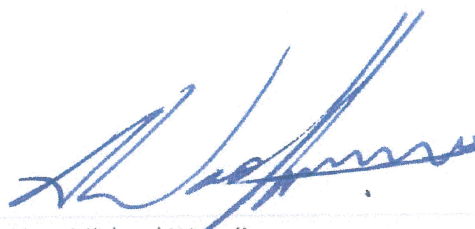
19.1 This DAA must be reviewed by the Ministers that have entered into this agreement within three years. Ministers are able to review this DAA without the requirement to wait for three years.

**Signed**



Hon Christopher Finlayson  
**Minister in Charge of the New Zealand  
Security and Intelligence Service**

Date Signed: 27/03/17



Hon Michael Woodhouse  
**Minister of Immigration**

Date Signed: 30/03/17

**UNCLASSIFIED**