



New Zealand
Security Intelligence
Service
Te Pā Whakamarumarū



Te Tari Taiwhenua
Internal Affairs

DIRECT ACCESS AGREEMENT

UNDER THE

INTELLIGENCE AND SECURITY ACT 2017

BETWEEN

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

AND

THE MINISTER OF INTERNAL AFFAIRS

RELATING TO

**DIRECT ACCESS BY NZSIS TO BIRTH, DEATH, MARRIAGE, CIVIL
UNION AND NAME-CHANGE INFORMATION HELD BY THE
REGISTRAR-GENERAL**

AND

**DIRECT ACCESS BY NZSIS TO CITIZENSHIP INFORMATION HELD BY
THE SECRETARY FOR INTERNAL AFFAIRS**

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 Internal Affairs (together the Parties).
- 1.2. This DAA comes into force on the date of the last signature.

2. Background and purpose

- 2.1. The Intelligence and Security Act 2017 (the ISA) enables an intelligence and security agency to have Direct Access to certain specified information contained on certain public sector databases.
- 2.2. The purpose of this agreement is to enable access by NZSIS (as an intelligence and security agency) to Registration Information held by the Registrar-General, and to Citizenship Information held by the Secretary for Internal Affairs.
- 2.3. The agreement is made under sections 125 and 130 of the ISA and covers access to the:
 - 2.3.1. **Birth Death and Marriages (BDM) Database** to collect and use Registration Information; and
 - 2.3.2. **Citizenship Database** to collect and use Citizenship Information.
- 2.4. This DAA replaces the previous DAA signed in December 2018.

3. Definitions

- 3.1. Terms relevant to this DAA are defined as follows:
 - 3.1.1. **Authorised Officers** means any NZSIS staff member (including NZSIS employees, officers, secondees, and integrated contractors) who:
 - 3.1.1.1. has been certified by NZSIS's Compliance Manager as having a legitimate need to access DIA Information in order to carry out any of NZSIS's statutory functions; and
 - 3.1.1.2. has completed all necessary training and certification requirements to access the databases.
 - 3.1.2. **Citizenship Information** means information that relates to the acquisition or loss of citizenship by, or to the citizenship status of, any person and does not include information as to any change of gender.
 - 3.1.3. **DIA Information** means Registration Information and/or Citizenship Information.
 - 3.1.4. **Direct Access**, in relation to the BDM and Citizenship Databases, means to do either or both of the following (whether remotely or otherwise):

- 3.1.4.1. Search the database; or
- 3.1.4.2. Copy any information stored on the database (including by previewing, cloning, or other forensic methods).
- 3.1.5. **International security standards for intelligence and security agencies** refers to the US Committee for National Security Systems Instruction 1253.
- 3.1.6. **Registration Act** means, as the context requires, the Births, Deaths, Marriages and Relationships Act 1995 or 2021 (both of which are to some extent in force at the time of signing of this agreement).
- 3.1.7. **Registrar-General**, means the Registrar-General appointed under the Public Service Act 2020 (as confirmed by section 79(1) of the Births, Deaths, Marriages, and Relationships Registration Act 1995 and section 124 of the Births, Deaths, Marriages, and Relationships Registration Act 2021).
- 3.1.8. **Registration Information:**
 - 3.1.8.1. means the following information as defined in section 2 of the Registration Act:
 - 3.1.8.1.1. Birth information
 - 3.1.8.1.2. Civil union information
 - 3.1.8.1.3. Death information
 - 3.1.8.1.4. Marriage information
 - 3.1.8.1.5. Name change information,
 - 3.1.8.2. does not include adoption information, witness protection name change information, sexual assignment or correction information to which ss 77(2), (3) or (4) of the Registration Act 1995 or s 107 of the 2021 Act applies, or Human Assisted Reproductive Technology Act 2004 donor or donor offspring information.
- 3.1.9. **Secretary** means the Secretary for Internal Affairs.
- 3.2. All of the other terms in this DAA have the meaning as described in the ISA unless otherwise noted.

4. Databases to be accessed

- 4.1. The databases to be accessed are:
 - 4.1.1. **BDM Database** means the series of statutory registers held by the Registrar-General in accordance with the Registration Act, which contain Registration Information.
 - 4.1.2. **Citizenship Database** means the series of statutory registers held by the Secretary in accordance with the Citizenship Act 1977 and regulations made under that Act which contain Citizenship Information.

5. Particular information that may be accessed

- 5.1. NZSIS may access Registration Information.
- 5.2. NZSIS may access Citizenship Information.

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

- 6.1. NZSIS will access DIA Information in support of its principal statutory objectives and the statutory functions specified in clause 7 of this agreement, for the following purposes:
 - 6.1.1. Identifying persons of security or intelligence interest and their familial details by obtaining and corroborating their biographical or familial details and/or the details of family members (i. e. intelligence collection and analysis);
 - 6.1.2. obtaining and corroborating the biographical or familial details of persons seeking a national security clearance, national security check or any other access, activity or appointment which requires NZSIS (or in which NZSIS is requested) to provide national security advice (i. e. protective security services, advice and assistance); and
 - 6.1.3. searching DIA Information to ensure NZSIS does not create or amend an assumed identity (or request the DIA to create or amend an assumed identity) which is an exact match with someone of the same name and birth date born in New Zealand;¹
 - 6.1.4. conducting searches in response to other information held by NZSIS. This includes target discovery, in which NZSIS would use indicators (or other relevant frameworks) to identify previously unknown individuals of concern.

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

- 7.1. DIA Information will be accessed by NZSIS for the following statutory functions, duties or powers:
 - 7.1.1. Intelligence collection and analysis;
 - 7.1.2. Protective security services, advice and assistance. The use of DIA Information in this regard by NZSIS includes but is not limited to:
 - 7.1.2.1. advice about national security risks (for example, in support of citizenship, immigration and border security decision-making processes);

¹ This includes conducting searches to ensure that NZSIS or the Government Communications Security Bureau (GCSB) does not create or amend an assumed identity which is an exact match with someone of the same name and birth date born in New Zealand.

- 7.1.2.2. supporting decision-making around the eligibility and suitability of individuals to be granted a national security clearance; and
 - 7.1.2.3. preventing, detecting and responding to risks to national security presented by individuals with access to sensitive or classified information; or
 - 7.1.3. Acquisition, use or maintenance of an assumed identity (for both NZSIS and the Government Communications Security Bureau (GCSB)) and requests for assistance to acquire, use and maintain an assumed identity (for both NZSIS and GCSB).
- 7.2. Additional information on how DIA Information will be used to support these functions, duties or powers is outlined in the Privacy Impact Assessment (PIA).

8. Mechanism by which information is accessed

- 8.1. NZSIS may have Direct Access to DIA Information through dedicated DIA terminals accessible only to Authorised Officers. Registration or Citizenship information must be assessed at the time of access as necessary for NZSIS purposes before it can be extracted, copied, and transferred to the NZSIS classified network.
- 8.2. Detailed mechanisms by which NZSIS may have Direct Access to DIA Information are set out in the PIA.
- 8.3. Any material changes to these access mechanisms or the PIA must be notified to the Inspector-General of Intelligence and Security (IGIS) and the Privacy Commissioner (PC).

9. Positions of persons who may access the information

- 9.1. Direct Access to Registration or Citizenship Information will be limited to persons who hold the position of Authorised Officer working directly on the functions, duties or powers specified in clause 7 of this DAA, and for the purposes specified in clause 6 of this DAA, where access is required to carry out that function, duty or power.
- 9.2. Prior to having Direct Access to DIA Information, each NZSIS Authorised Officer must:
 - 9.2.1. complete training on access to, use and disclosure of Registration Information as required by the Registrar-General, and Citizenship Information as required by the Secretary;
 - 9.2.2. complete training in legal and policy obligations relating to access to, use and disclosure of DAA information, and retention and record keeping obligations as required by the NZSIS Compliance Manager;
 - 9.2.3. undertake in writing that they:
 - 9.2.3.1. have completed the necessary training;
 - 9.2.3.2. understand and will comply with all of their obligations;
 - 9.2.3.3. will maintain the integrity of their individual access; and

9.2.3.4. will advise the NZSIS Compliance Manager if their need for access changes.

- 9.3. A Joint Standard Operating Procedure (**SOP**) whereby NZSIS's Authorised Officer requirements are set and managed, and unique access accounts are issued and deactivated has been finalised by DIA and NZSIS.
- 9.4. NZSIS will maintain an up-to-date and accurate record of the identities of all Authorised Officers, details of all training undertaken, and copies of all certifications.
- 9.5. DIA will only be advised of the NZSIS code for Authorised Officers, and will create pseudonyms for use within DIA systems.

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

- 10.1. Access to and use of DIA Information itself will generate detailed audit log data within the relevant BDM and Citizenship Databases.
- 10.2. NZSIS must keep an up-to-date and accurate record of:
- 10.2.1. Every occasion each Authorised Officer accesses Registration or Citizenship Information;
 - 10.2.2. The reason the Authorised Officer accessed the above information, and the necessity/justification for access; and
 - 10.2.3. Any records obtained by NZSIS from the relevant Database as a result of the search.
- 10.3. NZSIS must maintain a record of the above information in a way that can be audited by the Registrar-General or the Secretary if requested and will be made available to the Registrar-General to support the annual joint audit.
- 10.4. NZSIS, the Secretary and/or the Registrar-General (or their nominee) will undertake a joint audit of the operation of this DAA at least once per year, in accordance with a joint audit procedure. Should any previous audit identify issues of privacy concern the Registrar-General or Secretary should require a further joint audit within a reasonable time. A copy of this audit report will be provided to the IGIS, and any issues of privacy concern will be provided to the PC. Should there be any significant delay to the completion of the audit IGIS and PC will be advised by NZSIS.
- 10.5. The Registrar-General may review the access record at 10.2 at any time.
- 10.6. The Secretary may review the access record at 10.2 at any time.

11. Safeguards to be applied for protecting particular information

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

- 11.1.1.1. All Authorised Officers are security vetted to the highest level (Top Secret Special).
- 11.1.1.2. All Authorised Officers receive training on their privacy and official information obligations.
- 11.1.1.3. All Authorised Officers are subject to the NZSIS and Public Service Commission Codes of Conduct.
- 11.1.1.4. All Authorised Officers 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.
- 11.1.1.5. All access to and use of NZSIS electronic systems, is logged and monitored.

11.1.2. Access to DIA Information:

- 11.1.2.1. Only Authorised Officers may directly access DIA Information.
- 11.1.2.2. Authorised Officers may only access DIA Information in accordance with one of the purposes set out in clause 6 of this DAA.
- 11.1.2.3. Authorised Officers may only transfer DIA Information to the NZSIS database after determining that information to be necessary to one of NZSIS's functions, duties and powers specified in clause 7 of this DAA.

11.1.3. Safeguards for access to DIA Information obtained under this DAA and stored on NZSIS systems:

- 11.1.3.1. Access to DIA Information obtained under this DAA will be strictly controlled in accordance with international security standards for intelligence and security agencies.
- 11.1.3.2. DIA Information obtained under this DAA 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 and subject to audit as per clause 10.4.

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

- 12.1. All DIA Information obtained under this DAA 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. Any specific DIA Information that is copied into NZSIS systems and is used in support of NZSIS's statutory functions will be retained and managed as public records of NZSIS activities, in accordance with the Public Records Act 2005.

12.3. Disposal of DIA Information obtained under this DAA 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 Authorisation to NZSIS to share intelligence however that authorisation is classified. For the purposes of the DAA, it is sufficient to note that the Ministerial Authorisation authorises 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 DIA 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 be in compliance with all human rights obligations recognised by New Zealand law.

13.4. Disclosures of DIA 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. When considering whether to share any DIA Information, NZSIS must give due consideration to the Crown's relationships with Māori under the Treaty of Waitangi.

- 13.6. In addition to the above, when sharing intelligence with external parties NZSIS gives consideration to overarching principles as outlined in any relevant Ministerial Policy Statements (such as the MPS on Cooperation with overseas public authorities), any internal policy, including the need to consider whether the interaction aligns with NZSIS objectives and NZ 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 DIA'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 the Registration Act or Citizenship Act, however access to DIA 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 collecting, processing and storing Registration Information within the BDM Database remains the sole responsibility of the Registrar-General.
- 15.2. All costs associated with NZSIS's access to Registration Information within the BDM Database, including any costs associated with building a user interface, will be the joint responsibility of NZSIS and the Registrar-General.
- 15.3. All costs associated with collecting, processing and storing Citizenship Information within the Citizenship Database remains the sole responsibility of the Secretary.
- 15.4. All costs associated with NZSIS's access to Citizenship Information within the Citizenship Database, including any costs associated with building a user interface, will be the joint responsibility of NZSIS and the Secretary.
- 15.5. All costs associated with the collection of any information obtained under this DAA following its extraction from its respective database, as well as the subsequent processing, storage, access and disposal within NZSIS systems remains the sole responsibility of NZSIS.
- 15.6. All costs associated with dealing with a breach of this agreement will be met by the party responsible for the breach occurring.

16. Consultation with IGIS and PC

- 16.1. Before entering into this DAA, the Parties consulted with and invited comment from the IGIS and the PC. The Parties took into account and had regard to the comments by the IGIS and PC.

17. Publication of this agreement

- 17.1. This DAA will be published on the NZSIS and DIA websites.

17.2. The PIA will be published on the NZSIS and DIA websites.

18. Public's right of access

18.1. Nothing in this DAA affects an individual's right to make an information privacy request in accordance with the Privacy Act 2020 or to make a complaint to the Privacy Commissioner under the Privacy Act.

18.2. Nothing in this DAA affects an individual's right to make a complaint to the Inspector-General of Intelligence and Security in accordance with section 171 of the ISA.

18.3. All Parties agree to keep each other informed of any complaints arising from the use of the BDM Database or Citizenship Database relating to this agreement.

19. Dispute resolution

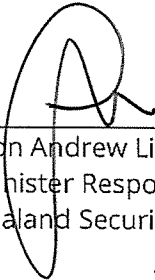
18.1 In the event of dispute the Parties will consult, through their nominated organisational representatives, with a view to resolving any issues as soon as practicable. If the dispute cannot be resolved, it will be escalated to the Chief Legal Advisor of DIA and the General Counsel of NZSIS or the Chief Executives for resolution.

18.2 Pending resolution of any dispute the Registrar-General or Secretary may, with a reasonable period of notice to NZSIS, suspend any Authorised Officer's access to their relevant database.

20. Review of this agreement

20.1. This DAA must be reviewed by the Minister Responsible for the NZSIS and the Minister of Internal Affairs within three years. This DAA can also be reviewed or amended (in accordance with the ISA) without the requirement to wait for three years.

Signed



Hon Andrew Little
Minister Responsible for the New
Zealand Security Intelligence Service

Date Signed: 29/9/22



Hon Jan Tinetti
Minister of Internal Affairs

Date Signed: 18/10/2022