



DIRECT ACCESS AGREEMENT

BETWEEN

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

AND

THE MINISTER OF CUSTOMS

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 Customs (“NZCS”) (“the Parties”).
- 1.2. This DAA comes into force upon the 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 public sector databases.
- 2.2. The purpose of this agreement is to enable access by NZSIS (as an intelligence and security agency) to the CusMod database, and the information contained within the database collected by NZCS (as the “holder agency”) under the Customs and Excise Act 2018.
- 2.3. 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. **Authorised Officers** means any NZSIS officer who has been certified by NZSIS’s Compliance Manager as a) having a legitimate need to access the CusMod database in order to carry out any of NZSIS’s statutory functions and b) having completed all of the necessary training and certification requirements to access the database.
 - 3.1.2. **Direct access**, in relation to a database, means to do either or both of the following (whether remotely or otherwise):
 - 3.1.2.1. Search the database (by way of the CusMod database query facilities);
 - 3.1.2.2. Copy any information stored on the database (including by previewing, cloning, or other forensic methods).
 - 3.1.3. **CusMod database**, means the database maintained by Customs, containing information about border-crossing persons, goods, and craft that has been collected in connection with the performance or exercise of a function, duty, or power under the Customs and Excise Act 2018.
 - 3.1.4. **NZCS information**, means all information recorded in the CusMod database listed in Schedule 2 ISA.

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 CusMod database.

5. Particular information that may be accessed

- 5.1. NZSIS may access all NZCS information recorded in the CusMod database, subject to any specific caveats placed on that information by NZCS.
- 5.2. Schedule 2 lists information about border crossing persons, goods, and craft that has been collected in connection with the performance or exercise of a function, duty, or power under the Customs and Excise Act 2018.

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

- 6.1. NZSIS will access the CusMod database in support of its principal statutory objectives and the statutory functions specified in section 7 of this agreement, for the following purposes:
- 6.1.1. creating, checking, retrieving, or managing automatic alerts; and
- 6.1.2. conducting searches in response to other information held by NZSIS.¹

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 the CusMod database to support the following statutory functions and powers, as specified in the ISA:
- 7.1.1. Intelligence collection and analysis;
- 7.1.2. Protective security services, advice and assistance. The use of CusMod database information in this regard by NZSIS includes but is not limited to: (a) advice about national security risks (for example, in support of immigration and border security decision-making processes); and (b) personnel security advice (for example security clearance assessments).
- 7.1.3. Acquiring, use or maintenance of an assumed identity (for both NZSIS and GCSB); and

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.

- 7.1.4. Request for assistance to acquire, use and maintain an assumed identity (for both NZSIS and GCSB).
- 7.2. Additional Information on how NZCS information will be used to support these functions is outlined in the classified Privacy Impact Assessment ("PIA").

8. Mechanism by which information is accessed

- 8.1. The NZCS information will be accessed through dedicated CusMod database terminals accessible to authorised NZSIS staff. Database information assessed at the time of access as relevant for NZSIS purposes will be extracted, copied, and transferred to the NZSIS classified network.
- 8.2. Detailed mechanisms by which NZCS information will be accessed by NZSIS are set out in the classified Privacy Impact Assessment ("PIA").
- 8.3. Any material changes to these access mechanisms or the PIA must be notified to the Inspector-General of Intelligence and Security and the Privacy Commissioner.

9. Positions of persons who may access the information

- 9.1. Access to the CusMod database will be limited to NZSIS Authorised Officers working directly on the functions specified in paragraph 7 of this agreement, where access is required to carry out that function.
- 9.2. Prior to accessing the CusMod database all NZSIS Authorised Officers must:
 - 9.2.1. Complete training regarding access to the CusMod database delivered by NZCS;
 - 9.2.2. Complete training in their legal and policy obligations relating to access and use of the CusMod database; retention, record keeping, and disclosure of that information accessed, delivered by NZSIS; and
 - 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 to CusMod databases; and
 - 9.2.3.4. will advise if their need for access to the CusMod database changes, or if any of the above 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 NZCS 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. NZCS will only be advised the NZSIS code for Authorised Officers, and will create pseudonyms for use within NZCS systems.

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

- 10.1. Access to and use of the CusMod database itself will generate detailed audit log data within NZCS systems.
- 10.2. NZSIS must keep an up-to-date and accurate record of:
 - 10.2.1. Every occasion each Authorised Officer accesses the CusMod database;
 - 10.2.2. The reason the Authorised Officer accessed the CusMod database, including entity/entities sought, and the justification for the access in all the circumstances; and
 - 10.2.3. Any records obtained by the NZSIS from the CusMod 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 NZCS if requested.
- 10.4. NZCS and NZSIS will undertake a joint audit of the operation of this DAA at least once per year, in accordance with a joint audit procedure. A copy of this audit report will be provided to the Inspector-General of Intelligence and Security, and any issues of privacy concern will be provided to the Office of the Privacy Commissioner.
- 10.5. NZCS can also review access by Authorised Officers to the CusMod database at any time.

11. Safeguards to be applied for protecting particular information

- 11.1. Detailed safeguards by which CusMod database 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 NZSIS employees are security vetted to the highest level (Top Secret Special).
 - 11.1.1.2. All NZSIS employees receive training on the Privacy and Official Information Acts.
 - 11.1.1.3. All NZSIS employees are subject to the NZSIS Code of Conduct.
 - 11.1.1.4. All NZSIS staff who have access to information directly accessed from the CusMod database must complete training on how to identify this information and the restrictions around its use

- 11.1.1.5. 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.
- 11.1.1.6. All access to and use of NZSIS electronic systems, is logged and monitored.
- 11.1.2. Access to the CusMod database
 - 11.1.2.1. Only NZSIS Authorised Officers may access the CusMod database directly.
 - 11.1.2.2. Authorised Officers may only transfer any record accessed in the CusMod database to the NZSIS database after determining that record to be relevant to NZSIS statutory functions.
 - 11.1.2.3. Any alert created within the CusMod database will be set to expire at a future date when information is expected to be no longer required.
 - 11.1.2.4. Alerts will be reviewed regularly to ensure that any alerts which cease to be relevant will be cancelled.
 - 11.1.2.5. Refer to paragraph 9 for further information on Authorised Officers.
- 11.1.3. Safeguards for access to information obtained from the CusMod database and stored on NZSIS systems
 - 11.1.3.1. Access to the information obtained from the CusMod database will be strictly controlled in accordance with international security standards for intelligence and security agencies.
 - 11.1.3.2. Information obtained from the CusMod database 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.

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

- 12.1. All information accessed from the CusMod 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. Any specific CusMod database 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 information obtained from the CusMod database 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 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 persons in specified circumstances.
- 13.3. In accordance with the ISA, NZSIS will only disclose NZCS 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 NZCS 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 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 NZCS's ability to disclose information under other provisions in the ISA or that is authorised or required under any enactment, or that is as permitted by the information privacy principles, however access to NZCS information via this DAA is to be preferred unless there is good reason to request the information via other means.

15. Apportionment of costs

15.1. All costs associated with collecting, processing and storing CusMod database information within NZCS-owned or controlled systems will be the sole responsibility of NZCS.

15.2. All costs associated with NZSIS access to the CusMod database within NZCS-owned or controlled systems, including any costs associated with building a user interface, will be the joint responsibility of the NZCS and the NZSIS.

15.3. All costs associated with the collection of information following its extraction from NZCS 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 NZCS and NZSIS websites.

16.2. The Privacy Impact Assessment will be published, but some information within it 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 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. 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: 20/10/21



Hon Meka Whaitiri
Minister of Customs

Date Signed: 18/10/2021