



**DIRECT ACCESS TO
THE NZCS CUSMOD DATABASE
BETWEEN
THE MINISTER IN CHARGE OF 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 in Charge of the New Zealand Security Intelligence Service ("NZSIS") and the Minister of Customs ("NZCS") ("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 NZCS CusMod database, and the information contained within the database collected by NZCS (as the "holder agency") under the Customs and Excise Act 1996.

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 NZCS 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 NZCS 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. **NZCS database** means the CusMod database, including:
 - 3.1.3.1. all of its computer components, including software, underlying data repositories, and any system interface required to access the database information; or
 - 3.1.3.2. any replacement database that fulfils similar functions.
- 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 NZCS database.

5. Particular information that may be accessed

5.1. NZSIS may access all information recorded in the NZCS database listed in Schedule 2 ISA, 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 1996.

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

6.1. NZSIS will access the NZCS 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.

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 NZCS database to support the following statutory functions, as specified in the ISA:

7.1.1. Intelligence collection and analysis;

7.1.1 Protective security services, advice and assistance. The use of NZCS 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).

7.2 Additional Information on how NZCS database 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 database will be accessed through dedicated NZCS database terminals accessible to authorised NZSIS staff. Database information accessed 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 the NZCS database will be accessed by NZSIS are set out in the classified Privacy Impact Assessment ("PIA"). This will be updated as appropriate, and the Privacy Commissioner and the Inspector-General of Intelligence and Security will be notified of any material changes.

9. Positions of persons who may access the information

9.1. Access to the NZCS 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 NZCS database all NZSIS Authorised Officers must:

- 9.2.1. Complete training regarding access to the NZCS database delivered by NZCS;
- 9.2.2. Complete training in their legal and policy obligations relating to access and use of the NZCS 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 NZCS databases; and
 - 9.2.3.4. will advise if their need for access to the NZCS database changes, or if any of the above changes.
- 9.3. NZSIS and NZCS will agree in writing to a mechanism whereby NZSIS's Authorised Officer requirements are set and managed, and unique access accounts are issued and deactivated.
- 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 NZCS 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 NZCS database;
 - 10.2.2. The reason the Authorised Officer accessed the NZCS database, including entity/entities sought, and justification of access in light of less intrusive datasets and privacy impacts; and
 - 10.2.3. Any records obtained by the NZSIS from the NZCS 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 NZCS database at any time.

11. Safeguards to be applied for protecting particular information

11.1. Detailed safeguards by which NZCS 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 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.
- 11.1.1.5. All access to and use of NZSIS electronic systems, is logged and subject to system auditing to ensure that access to information is in accordance with legislative requirements, NZSIS policies, and the individual employee's role.

11.1.2. Access to the NZCS database

- 11.1.2.1. Only NZSIS Authorised Officers may access the NZCS database directly.
- 11.1.2.2. Authorised officers may only access the NZCS database in respect of a pre-identified entity.
- 11.1.2.3. Authorised Officers may only transfer any record accessed in the NZCS database to the NZSIS database after determining that record to be relevant to NZSIS statutory functions.
- 11.1.2.4. Any alert created within the NZCS database will be set to expire at a future date when information is expected to be no longer required.
- 11.1.2.5. Alerts will be reviewed regularly to ensure that any alerts which cease to be relevant will be cancelled.
- 11.1.2.6. Refer to paragraph 9 for further information on Authorised Officers.

11.1.3. Safeguards for access to information obtained from the NZCS database and stored on NZSIS systems

- 11.1.3.1. Access to the information obtained from the NZCS database will be strictly controlled in accordance with international security standards for intelligence and security agencies.
- 11.1.3.2. Information obtained from the NZCS 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 NZCS 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 NZCS 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, with a default retention period of 25 years.
- 12.3. Disposal of information obtained from the NZCS 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 Intelligence and Security Act provides in section 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 section 13 authorisation and the relevant Ministerial Policy Statement. NZSIS will advise NZCS of any changes in obligations with regards to disclosure of information arising from any section 13 authorisation and/or Ministerial Policy Statement.
- 13.3. In relation to overseas persons, NZSIS may provide NZCS database information and any analysis of that information (together "CusMod-Related Intelligence" or "CRI") 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 CRI to another 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 CRI should be provided, having regard to:
 - 13.3.1. the nature and scope of the CRI NZSIS proposes to provide;
 - 13.3.2. the nature of the agency to which NZSIS proposes to provide the CRI; and
 - 13.3.3. whether provision of the CRI 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 CRI to New Zealand Government entities. In the event the Director of Security determines it is in the interests of security to provide CRI 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 CRI should be provided, having regard to:

- 13.4.1. the nature and scope of the CRI NZSIS proposes to provide;
 - 13.4.2. the nature of the agency to which NZSIS proposes to provide the CRI; and
 - 13.4.3. whether provision of the CRI 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 CRI 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 CRI 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:
- 13.7.1.1. that it is necessary to share CRI 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
 - 13.7.1.2. it is not possible to obtain the prior approval of the Minister due to the urgent nature of the imminent threat;
- the Director of Security may authorise the sharing of CRI 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 CRI 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 collecting, processing and storing NZCS 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 NZCS 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 is classified so will not be published, and may be withheld as authorised by section 107(2)(b) of the ISA and in accordance with the Official Information Act 1982.

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 an individual's right 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.

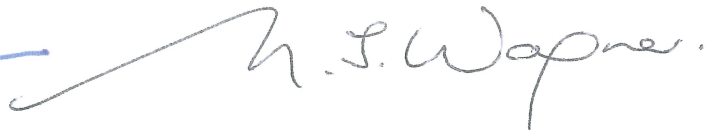
Signed



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

Date Signed:

28 March 2017



Hon Nicky Wagner
Minister of Customs

Date Signed:

27/3/2017,