New Zealand Security Intelligence Service
Te Pā Whakamarumaru

New Zealand Customs Service (NZCS) CusMod Information

Privacy Impact Assessment Report

Owner	Knowledge Manager
Approved By	Chief Privacy Officer
Approval Date	20 October 2021
Review Date	20 May 2024

Contents

Part 1: Relevant Legislation

1. Under section 125(1) and Schedule 2 of the Intelligence and Security Act (ISA) 2017, the New Zealand Security Intelligence Service (NZSIS) is authorised to have direct access to certain information held by other agencies.

2. An update to the Direct Access Agreement (DAA) between NZSIS and New Zealand Customs Service (NZCS) came into effect on 20 October 2021 after being signed by both parties on 20 October 2021 and enables NZSIS to access 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, which is held in the CusMod database. [1]

Part 2: NZSIS Responsibilities

3. NZSIS direct access to CusMod information must comply with the terms of the DAA, as signed by the Minister responsible for Customs and the Minister responsible for NZSIS.[2]

Using CusMod information

4. In accordance with terms of the DAA and the legislative requirements of the ISA, NZSIS must ensure that

    i. any data provided by NZCS via direct access is used[3] only for the purposes of NZSIS statutory functions as set out in the ISA; and

    ii. any data obtained directly from the CusMod database is used in a way that is necessary and proportionate to NZSIS functions.

Protecting CusMod information

5. In accordance with terms of the DAA and the legislative requirements of the ISA, NZSIS must ensure there are adequate safeguards in place to protect CusMod information. This includes ensuring that there are

    i. clear procedures for accessing, using, disclosing and retaining CusMod information;

    ii. clear measures for protecting the privacy of individuals identified by CusMod information; and

    iii. sufficient compliance and audit requirements for the direct access, use, disclosure, and retention of Customs information.

6. For a more detailed description of the ways in which NZSIS will fulfil these responsibilities, see Part 4: Use of CusMod information and Part 5: Protecting CusMod information.

---

[1] Any reference to CusMod or the CusMod database can be taken to be a reference to the information asset that is known as CusMod, and includes:
   a. the data held in the CusMod database; or
   b. all of its computer components, including software, underlying data repositories, and any system interface required to access the database information.

[2] Before entering into a DAA, both Ministers must be satisfied that direct access to the information is necessary to enable NZSIS to perform any of its functions, there are adequate safeguards to protect the privacy of individuals and the agreement will include appropriate procedures for direct access, use, disclosure, and retention of the information.

[3] 'Access to' or 'use of' CusMod information includes any activity requiring the user to log in to the NZCS CusMod system, even if the only action is the log in itself.

NZSIS ownership

7. For a comprehensive list of NZSIS employees responsible for ensuring NZSIS is compliant with the obligations outlined in the DAA, refer to Appendix 1.

Part 3: Scope

In scope

8. This Privacy Impact Assessment (PIA) report should be read in conjunction with the updated DAA between NZSIS and New Zealand Customs Service. This PIA report

    i. identifies the privacy concerns and considerations associated with NZSIS having direct access to CusMod information; and

    ii. outlines the ways in which NZSIS will access, use and protect CusMod information in order to adequately mitigate these privacy concerns.[4]

Out of scope

9. This PIA does not cover any potential access to CusMod information by the Government Communications Security Bureau (GCSB) or any other agency.

Part 4: Use of CusMod information

10. While CusMod information is collected primarily for the purposes of maintaining New Zealand's border security, NZSIS utilises CusMod information for the purposes of maintaining and enhancing New Zealand's national security.

NZSIS will only use CusMod information to fulfil its statutory functions

11. NZSIS uses CusMod information to fulfil the following statutory functions of the organisation: :

    a. protective security services, advice and assistance; and

    b. intelligence collection and analysis.

Providing protective security services, advice and assistance to partner agencies

12. NZSIS may access CusMod information for the purposes of providing protective security services, advice and assistance to partner agencies. This activity includes, but is not limited to:

    i. undertaking security clearance assessments (vetting);and

    ii. providing advice about national security risks at the request of partner agencies.[5]

Intelligence collection and analysis

13. In support of its Intelligence Collection and Analysis function, NZSIS will conduct investigative analysis using CusMod: user-driven searches of CusMod information to meet general investigative, operational and security requirements.

[4] This covers the entirety of the information management lifecycle (receipt, storage, access, use, retention and disposal) of CusMod data by NZSIS.

[5] For example, responding to Advance Passenger Processing (APP) alerts for the purposes of protecting border security; providing national security advice correspondence to partner agencies such as Immigration New Zealand (INZ), Department of Internal Affairs (DIA) and Ministry of Foreign Affairs (MFAT) in support of their decision making functions for visa, citizenship, refugee and/or diplomat applications; providing security checks to New Zealand Police to enhance the security planning for major events such as APEC, Rugby World Cup etc.

14. NZSIS staff utilise CusMod information to help further investigations into people of national security.

15. Investigative Analysis may also be undertaken on CusMod information to complete discovery projects and generate further investigative leads. This allows NZSIS to identify additional actions NZSIS should undertake to maintain/protect the national security of New Zealand.

16. Staff will also use CusMod to assist in meeting collection objectives, namely scoping, planning, carrying out and providing support to proposed or ongoing operational activity.

NZSIS will use CusMod information in a way that is necessary and proportionate

17. NZSIS will only use CusMod information when it is reasonably necessary for the purposes of undertaking our specific statutory function(s).[6]

18. The way in which the NZSIS uses CusMod information must be proportionate to the activity we are undertaking. The benefit of using the CusMod information for the purposes of undertaking NZSIS' statutory functions must outweigh the potential intrusion of privacy that may result from NZSIS acquiring and retaining the dataset.

Part 5: Protecting CusMod information

Secure data ingestion and storage

19. NZSIS access CusMod information from Customs via stand-alone CusMod terminals. The terminals operate on a fully encrypted virtual private network (VPN) hosted on the all-of-government one.govt network. The VPN provides an additional layer of security and encryption for CusMod information, above the standard security provided by using the one.govt network.

20. CusMod information assessed as relevant to NZSIS' statutory functions is manually transferred by the Authorised Officer to NZSIS's fully security accredited Top Secret network for processing, storage and future use.

21. Access to the NZSIS network is strictly controlled in accordance with New Zealand and Five Eyes security standards for Top Secret networks. It is only accessible by staff who have been security vetted to the highest level (Top Secret Special).

Access to CusMod information

22. NZSIS staff may access CusMod information in two ways

    i. direct to CusMod information via a CusMod terminal; and

    ii. access to CusMod information which has been ingested into NZSIS intelligence systems.

[6] NZSIS functions include intelligence collection and analysis, protective security services, advice and assistance, information assurance and cybersecurity services, cooperation with other public authorities to facilitate their functions and cooperation with other entities to respond to imminent threat.

23. Not all NZSIS staff have access to CusMod information. Both access methods have unique access restriction mechanisms, to ensure CusMod information is accessed by those authorised to do so for the purposes of undertaking NZSIS' statutory functions.

Direct access to CusMod information via a CusMod terminal

24. Direct access to CusMod information via a CusMod terminal is limited to Authorised Officers only.

25. Authorised Officers are those employees issued with a designated user profile and log-in credentials for the CusMod terminal. The number of user profiles is limited and additional profiles are subject to approval by both NZSIS and NZCS.

26. NZSIS has clear operational procedures for Authorised Officers regarding when and how they may use the CusMod terminal.

Access to CusMod information held within NZSIS intelligence systems

27. Access to CusMod information held within NZSIS systems is limited to NZSIS employees working directly in intelligence and security roles[7] as well as a small number of staff in enabling functions (compliance, information management, legal advisors, IT administration, etc.). This access is not authorised until the employee has successfully completed mandatory Direct Access compliance training, obtained sign off from their Line Manager and confirmation from the NZSIS Compliance and Risk team.

Access auditing

28. User access to CusMod information is captured in two ways

    i. the CusMod Register of Use for information accessed via a CusMod terminal; and

    ii. automated audit log data for CusMod information accessed via NZSIS intelligence systems.

29. **CusMod Register of Use:** each instance of access[8] to CusMod information via a CusMod terminal must be recorded in the CusMod Register of Use by the Authorised Officer. Failure to record activity in the CusMod Register of Use may result in a breach of the conditions of use of CusMod, which may result in the termination of the Authorised Officer's CusMod account and/or access privileges.

30. The CusMod Register of Use is audited by the NZSIS Compliance and Risk team on an annual basis to ensure that Authorised Officers are compliant with CusMod record keeping requirements. NZSIS also provide the CusMod Register of Use to NZCS on an annual basis for additional auditing against NZCS system records. Any misuse of the CusMod system, including inappropriate access to CusMod information by an NZSIS employee, will be reported to the Inspector General of Intelligence Services (IGIS) in line with NZSIS processes for compliance incidents.

31. **Automated audit logs:** All access to CusMod by NZSIS staff is monitored by the NZCS. Audit data is used to support security and compliance auditing.

[7] This includes security clearance vetting.
[8] 'Access' refers to any activity requiring the user to log in to the NZCS CusMod system; this includes each CusMod search undertaken by the Authorised Officer **and** also captures the action of the log in itself.

Disclosure of CusMod information to other parties

32. Authorised Officers must not access CusMod information on behalf of other agencies, except as part of a statutory NZSIS function.

33. CusMod information may be provided to other New Zealand government departments or overseas intelligence partners by virtue of it being incorporated into an intelligence report.[9] Any such information sharing will be conducted in accordance with the CusMod Direct Access Agreement, as well as Ministerial Policy Statements and NZSIS policies.

Retention/archive/deletion of CusMod information

34. NZSIS will fulfil its statutory obligations and act in accordance with any Ministerial Policy Statement regarding the retention and disposal of data.

Retaining CusMod information

35. Information which has been retrieved from CusMod and is required to support the statutory functions of NZSIS is ingested into NZSIS's intelligence analysis system and managed as a business record of NZSIS activities.

Deleting/Archiving CusMod information

36. All NZSIS business records are subject to an agreed disposal authority (DA692) that was issued by the Chief Archivist in September 2020.

Part 6: Privacy risks and mitigations

37. The table below outlines the privacy risks associated with NZSIS's access to CusMod information and the steps that NZSIS will take to mitigate these risks. The residual risk rating assigned to each risk is assessed using the NZIC Joint Risk Management Framework outlined in Annex 2.

[9] For example to verify an individual's identity or in support of joint investigative work.

RISK 1
Insecure transfer or storage of CusMod information, leading to access by an unauthorised external person

Impacts	*Summary of mitigations*
CusMod information captures a large volume of personal and travel information about New Zealand citizens and foreign nationals. Unauthorised access to this information by an external party (a member of the public or a hostile foreign intelligence service hacking into the information) may result in the following impacts • a major breach of the Privacy Act • significant negative impact on public trust and confidence in NZSIS and the reputation of NZSIS • significant negative impact on the relationship between NZSIS and Customs • possible that CusMod information could be used by a hostile actor to enhance their own capabilities and/or undermine the national security of New Zealand	NZSIS takes extensive steps to ensure CusMod information is transferred and stored securely. **Data transfer** • transfer of CusMod information from Customs to NZSIS is conducted via a dedicated, encrypted virtual private network (VPN) link over the all-of-government one.govt network • the VPN provides an additional layer of security and encryption for CusMod information, above the standard security provided by using the one.govt network. **Data storage + systems access** • all CusMod information retention and access is conducted on NZSIS's Top Secret network • access to the NZSIS network is strictly controlled in accordance with New Zealand and Five Eyes security standards for Top Secret networks • access is only granted to people working for NZSIS, all of whom have been security vetted to the highest level (Top Secret Special) **Systems Certification and Accreditation (C&A)** • the NZSIS network is classified at TOP SECRET (the highest level of government network security) and is fully security accredited by GCSB **Access auditing** • all access by NZSIS staff (including system administrator access) to CusMod information generates detailed audit log data, and this will be the same for investigative analysis searches conducted on CusMod information • this audit log data is available to support security and compliance auditing, both by NZSIS security officers and the IGIS

Residual Risk Rating		
Likelihood: RARE	Impact: CRITICAL	Residual Risk Rating: **MEDIUM**

RISK 2
Unauthorised and/or inappropriate access to CusMod information by an NZSIS employee

Impacts	***Summary of mitigations***
CusMod information captures a large volume of personal and travel information about New Zealand citizens and foreign nationals. Unauthorised and/or inappropriate access to CusMod information by an NZSIS employee may have a range of impacts, depending on the nature and the extent of access. This could include, but is not limited to • a moderate breach of the Privacy Act • moderate impact on public trust and confidence in NZSIS and the reputation of NZSIS • minor impact on the relationship between NZSIS and Customs 'Access' or 'use' of CusMod includes any activity requiring the user to log in to the NZCS CusMod system, even if the only action is the log in itself.	NZSIS takes extensive steps to ensure CusMod is only accessed by authorised NZSIS employees for appropriate purposes. ***Systems mitigations*** **Access to the CusMod terminal (Authorised Officer)** • access to CusMod information is strictly limited to Authorised Officers only; an 'Authorised Officer' means anyone working for NZSIS who has been certified by NZSIS's Compliance Manager as having a legitimate need to access the NZCS database in order to carry out any of NZSIS's statutory functions having completed all of the necessary training and certification requirements to access the database. **Access to CusMod information held in NZSIS systems is limited by Access Control Group (ACG) settings** • NZSIS intelligence analysis systems limit access to CusMod information to NZSIS staff who have received training in the identification of data obtained by direct access and who have signed a briefing acknowledging their responsibilities in respect of this information. **Access auditing** • the Authorised Officer must record each search they undertake in the CusMod database in the CusMod Register of Use • the CusMod Register of Use is maintained by the NZSIS Compliance and Risk team and is audited on an annual basis to ensure that Authorised Officers are compliant with the record keeping requirements outlined in *NZSIS Policy – Direct Access to the NSCS CusMod Database* and *ID – Using the CusMod System SOP* • NZSIS will provide the CusMod Register of Use to NZCS on an annual basis for additional auditing against NZCS system records, to ensure NZSIS access to CusMod is in keeping with the DAA • any misuse of the CusMod system, including inappropriate access to CusMod information by an NZSIS employee, will be reported to the Inspector General of Intelligence Services (IGIS) in line with NZSIS processes for compliance incidents • failure to record use could result in a breach of the conditions of use of CusMod and termination of the user's and/or NZSIS's access privileges. ***Operational mitigations*** **Training** • all NZSIS staff must complete information management training, including training on their responsibilities in searching for and accessing information appropriately. this training also makes NZSIS employees aware of their information management obligations under the Intelligence and Security Act 2017, the Public Records Act, the Privacy Act, the Official Information Act and the Ministerial Policy Statement (MPS) on information management

- Specific training on identifying Direct Access information is mandatory for all NZSIS staff who need to access intelligence information as part of their role
- Intelligence Analysts receive additional role-specific training, which includes detailed instruction relating to accessing and using CusMod information

Managerial oversight

- NZSIS managers are responsible for ensuring employees are aware of their obligations and only access information that is reasonably required to enable them to carry out their official duties as part of NZSIS's functions

Compliance and monitoring

- NZSIS Privacy Officers are responsible for advising the Director of Security and the SLT on the adequacy of NZSIS systems for dealing with personal information and compliance with the Privacy Act and steps to be taken to promote robust privacy practices.
- a dedicated NZSIS Compliance Team oversees the development, implementation and compliance with relevant policies, including information management and access policies
- NZSIS has a dedicated security team with full access to all audit log data, whose responsibilities include investigating anomalous access to any NZSIS information
- unauthorised and/or inappropriate access to CusMod information will be treated as a security breach.
- Where an internal investigation confirms a privacy breach, and it is considered necessary or required by law,[10] the relevant affected parties (including NZSIS) and/or the Office of the Privacy Commissioner will be notified as soon as possible. NZSIS will also inform the Inspector General of Intelligence and Security.

Strategic mitigations

Policies, Standard Operating Procedures (SOPs) and user agreements

- all NZSIS employees with access to CusMod information must comply with the access and usage requirements outlined in NZSIS Policy and SOP documentation, which reflect the requirements of the CusMod Direct Access Agreement
- all NZSIS employees must read and sign an Information Technology and Information Systems Agreement for General Users
- all NZSIS employees must read and sign the NZSIS Code of Conduct, which outlines requirements for access to sensitive information contained within NZSIS systems
- failure to comply with NZSIS policies, SOPs, user agreements and/or the NZSIS code of conduct will be investigated and may result in disciplinary action.

Internal work programmes

[10] For example Section 114 of the Privacy Act 2020 requires mandatory notification to the Privacy Commissioner as soon as practicable after an agency becomes aware that a notifiable privacy breach has occurred.

	• NZSIS has an ongoing work programme regarding unauthorised and/or inappropriate access to information that includes reviewing user and system administrator accesses to ensure the appropriate level of restrictions are in place; ongoing review and improvement of security controls relating to access/removal of information from NZSIS systems; and reviewing audit log data requirements relating to system usage.		
	Residual Risk Rating		
	Likelihood: RARE	Impact: MODERATE	Residual Risk Rating: **LOW**

RISK 3
Unauthorised and/or inappropriate sharing of CusMod information with a domestic or international agency

Impacts	*Summary of mitigations*
Sharing CusMod information with external agencies (both domestic and international) is routine practice for NZSIS. NZSIS share CusMod information with external agencies in order to meet a range of operational requirements, including • to verify an individual's identity • to obtain further details, or • to progress joint national security investigations. Unauthorised and/or inappropriate sharing of CusMod information with an external agency may have a range of impacts depending on what information is shared and who it is shared with. This could include, but is not limited to • a major breach of the Privacy Act • significant negative impact on public trust and confidence in NZSIS and the reputation of NZSIS • significant negative impact on the relationship between NZSIS and Customs	NZSIS takes extensive steps to ensure all information shared with external agencies, including CusMod information obtained via direct access, is shared in a way that is authorised and appropriate. **Training** • NZSIS staff employees must complete mandatory training regarding Information Management and Human Rights • NZSIS employees must complete the Information Management training module as soon as possible following induction. NZSIS employees who regularly interact with overseas parties with must complete Human Rights risk management training following induction and must refresh their training on an annual basis; these training modules outline the human rights risk management policy which applies to the activities of NZSIS, and details how this policy is applied when data is shared with international agencies. **Procedural mitigations** • CusMod information may only be provided by NZSIS to other New Zealand government departments or overseas intelligence partners in accordance with the Intelligence and Security Act 2017 (ISA), NZSIS policies and SOPs • NZSIS Managers are responsible for ensuring that any information released to external agencies (both foreign and domestic) meets NZSIS information sharing requirements. Any unauthorised and/or inappropriate sharing of information derived from CusMod with an external agency would be treated as a security breach and prompt an investigation, in which NZCS would be consulted. Security breach investigations may lead to disciplinary action. **Systems mitigations** • NZSIS can only share information with external agencies via secure information sharing mechanisms • all information sharing mechanisms generate detailed audit log data, which is available to support security and compliance auditing • physical transfer of information off the network for the purposes of sharing the information with an external agency must be authorised and comply with NZSIS information security standards

Residual Risk Rating		
Likelihood: RARE	Impact: MODERATE	Residual Risk Rating: **LOW**

RISK 4
CusMod information is retained for longer than necessary within NZSIS systems

Impacts	*Summary of mitigations*

Retention of CusMod information (and therefore personal information) for longer than necessary would be contrary to IPP9 and may constitute a moderate breach of the Privacy Act.	All CusMod data that is brought into the NZSIS intelligence analysis system is information that has featured in a legitimate NZSIS function, and is maintained as a business record in accordance with our agreed disposal schedule (DA692).		
	Residual Risk Rating		
	Likelihood: UNLIKELY	Impact: MINOR	Residual Risk Rating: **LOW**

Part 7: Compliance and Audit Requirements

38. NZCS and NZSIS will undertake a joint audit of the operation of this DAA at least once per year, in accordance with a jointly agreed audit procedure. A copy of this audit report will be provided to the Inspector-General of Intelligence and Security and the Office of the Privacy Commissioner.

39. NZCS can also review access by Authorised Officers to CusMod at any time.

40. The information provided to NZCS will not include details of NZSIS operations and investigations, but will include the statutory functions being exercised and the purposes for which CusMod was accessed.

ENDS

Appendix 1: NZSIS Roles and Responsibilities

1. The **Director of Security** is responsible for ownership of all NZSIS information assets, with the authority to delegate ownership to the Knowledge Manager.

2. The **Knowledge Manager** is responsible for:

    i. the management and flow of information, including CusMod information management;

    ii. ensuring the risk mitigations outlined in this Privacy Impact Assessment (PIA) report are implemented across NZSIS; and

3. The **NZSIS Chief Privacy Officer** is responsible for:

    i. advising NZSIS Senior Leadership on the adequacy of NZSIS systems for storing, managing and protecting CusMod information;

    ii. monitoring compliance with the Privacy Act, in conjunction with the Compliance and Risk Manager;

    iii. promoting robust privacy practices across NZSIS; and

    iv. overseeing investigations into complaints lodged with the Privacy Commissioner regarding NZSIS access to or use of CusMod information.

4. The **Principal Advisor Joint Strategy, Performance and Policy** is responsible for:

    i. managing and responding to Official Information Act (OIA) requests and Privacy Act requests on behalf of NZSIS; and

    ii. managing privacy issues in conjunction with other relevant business units.

5. The **Compliance and Risk Manager is responsible for:**

    i. maintaining the acting as the operational lead for access to and use of CusMod information by NZSIS teams; and

    ii. liaising with NZ Customs Risk and Integrity staff to conduct the annual joint audit of NZSIS access to CusMod.

Appendix 2: Privacy Principles

6. NZSIS will take all reasonable and necessary steps to minimise the privacy impacts associated with the ingestion and use of CusMod information obtained under the Direct Access Agreement (DAA) in order to

    i. fulfil our obligations under the DAA;

    ii. fulfil our obligations under the Privacy Act;

    iii. maintain credibility and public confidence in NZSIS' privacy standards.

7. Table 1 provides an assessment of NZSIS' compliance with the 13 privacy principles outlined in the Privacy Act 2020, in relation to the use of CusMod information obtained under the DAA for NZSIS' statutory functions.

Table 1. NZSIS Privacy Principles Assessment

	Privacy Principle as per the Privacy Act	NZSIS assessment against privacy principle	Compliance with Privacy Principle?

1	**Purpose of the collection of personal information** *Collection of personal information by an agency must be lawful and necessary to the function of the agency*	NZSIS has access to CusMod information for the purpose of undertaking its statutory functions. NZSIS access to CusMod information is **lawfully** authorised under the Schedule 2 of the Intelligence and Security Act (ISA) 2017. Information is considered **necessary** where it is required to support the performance of NZSIS' statutory functions • intelligence collection and analysis • protective security services, advice, and assistance • co-operation with other public authorities to facilitate their functions • co-operation with other entities to respond to imminent threat	Compliant

2	**Source of personal information** *Get it directly from the people concerned wherever possible.*	If NZSIS were to collect CusMod information from the individual, this may • be prejudicial to the maintenance of the law; • prejudice the purposes of the collection; and • would not be reasonable practicable in the circumstances NZSIS is exempt from PP2 under s28 of the Privacy Act; however NZSIS access to CusMod information via Customs is lawful as per Schedule 2 of the ISA.	Exempt under s28 of the Privacy Act
3	**Collection of information from subject** *Tell them what information you are collecting, what you're going to do with it, whether it's voluntary, and the consequences if they don't provide it.*	The DAA between Customs and NZSIS is publically available and makes it clear that NZSIS has access to CusMod information collected by Customs. While it is public knowledge that NZSIS have **access** to CusMod information, details of exactly how NZSIS **uses** CusMod information are not available to the public in order to protect national security practices. For this reason, NZSIS is exempt from PP3 under s28 of the Privacy Act.	Exempt under s28 of the Privacy Act

4	**Manner of collection of personal information** Personal information shall not be collected by an agency (a) by unlawful means; or (b) by means that, in the circumstances of the case (i) are unfair; or (ii) intrude to an unreasonable extent upon the personal affairs of the individual concerned. *Be fair and not overly intrusive in how you collect the information*	PP4(a): NZSIS access to CusMod information is lawful as per Schedule 2 of the ISA PP4(b): NZSIS access to CusMod information is exempt from PP4(b) under s28 of the Privacy Act	Compliant with PP4(a) Exempt from PP4(b) under s28 of the Privacy Act
5	**Storage and security of personal information** *Take care of it once you've got it and protect it against loss, unauthorised access, use, modification or disclosure and other misuse*	All CusMod information is ingested and stored on a fully security accredited Top Secret network. NZSIS take extensive measures to ensure storage and access to CusMod information is secure.	Compliant
6	**Access to personal information** *People can see their personal information if they want to*	Under the Privacy Act and the Official Information Act, an individual has the right to seek confirmation from both Customs and NZSIS about whether personal information is held about them. Customs are responsible for the collection of CusMod information from the source. As the "holder agency", Customs are best place to handle information requests from individuals regarding their CusMod information. Any personal and/or official information requests to NZSIS regarding CusMod information will be transferred to NZCS. Any CusMod information that is brought into the main NZSIS intelligence analysis system following an investigative analysis query will be considered by NZSIS through their standard information request process.	Compliant
7	**Correction of personal information** *They can correct it if it's wrong, or have a statement of correction attached.*	Under the Privacy Act and the Official Information Act, an individual has the right to request that their personal information is amended if it is incorrect. As the "holder agency", Customs are best place to handle requests from individuals regarding corrections to their CusMod information. Any requests to NZSIS regarding corrections to an individual's CusMod information will be transferred to NZCS.	Compliant
8	**Accuracy etc. of personal information to be checked before use** *Make sure personal information is correct, relevant and up to date before you use it*	Customs have established procedures with air carriers to ensure the accuracy of CusMod information (most notably that all personal information must be as shown in the individuals' passport of certificate of identity). NZSIS operational procedures require employees to undertake rigorous analysis of the individual's case against intelligence holdings to confirm their identity **before** acting on CusMod information.	Compliant
9	**Not to keep personal information for longer than necessary** *Get rid of it once you're done with it.*	Any CusMod information that is brought into the main NZSIS intelligence analysis system following an investigative analysis query is maintained as a business record of NZSIS, with disposal arrangements as agreed in disposal authority DA692.	Compliant

10	**Limits on use of personal information** *Use it for the purpose you collected it for, unless one of the exceptions applies.*	PP10 states that an intelligence and security agency that holds personal information that was obtained in connection with one purpose may use the information for any other purpose (a secondary purpose) if the agency believes on reasonable grounds that the use of the information for the secondary purpose is necessary to enable the agency to perform any of its functions. The use of CusMod information for protective security functions and intelligence collection and analysis is necessary to enable NZSIS to perform its statutory functions. This use is therefore permitted under exemptions under IPP10, including (c)(i) to avoid prejudice to the maintenance of the law; (d) public health or public safety; (e) directly related to the purpose in connection with which the information was obtained.	Compliant
11	**Limits on disclosure of personal information** *Only disclose it if you've got a good reason, unless one of the exceptions applies*	Under s10 of the ISA, NZSIS is authorised to provide any intelligence collected and any analysis of that intelligence to the Minister, the Chief Executive of DPMC, and any person or class of persons (whether in New Zealand or overseas) authorised by the Minister to receive the intelligence and any analysis. Under section 11 of the ISA, NZSIS is authorised to, amongst other things, provide advice and assistance to any public authority (whether in New Zealand or overseas), any person or class of persons (whether in New Zealand or overseas) authorised by the Minister. This protective security services, advice, and assistance includes for the purposes of providing advice and assistance around personnel, information, and physical security, as well as advice around national security risks. Under s13 of the ISA, NZSIS is authorised to cooperate with other New Zealand government departments Under section 14 of the ISA, NZSIS is authorised to provide advice and assistance to anyone responding to an imminent threat to the life or safety of any person in New Zealand, or any New Zealand citizen or permanent resident overseas, any person in any area that New Zealand has search and rescue responsibilities for, or any person outside the territorial jurisdiction of any country. Any information sharing undertaken by NZSIS is conducted in accordance with the DAA, as well as Ministerial Policy Statements and NZSIS policies. Disclosure of personal information by NZSIS comes within the following exemptions to IPP11: (a) disclosure is one of the purposes (or directly related) for which information was obtained; (e) non-compliance is necessary to avoid prejudice to the maintenance of the law or for Court proceedings; (f) necessary to prevent or lessen a serious threat. (g) that the disclosure of the information is necessary to enable an intelligence and security agency to perform any of its functions.	Compliant

12	**Disclosure of personal information outside New Zealand**	Under s10 of the ISA, NZSIS is authorised to provide any intelligence collected and any analysis of that intelligence to the Minister, the Chief Executive of DPMC, and any person or class of persons (whether in New Zealand or overseas) authorised by the Minister to receive the intelligence and any analysis. Under section 11 of the ISA, NZSIS is authorised to, amongst other things, provide advice and assistance to any public authority (whether in New Zealand or overseas), any person or class of persons (whether in New Zealand or overseas) authorised by the Minister. This protective security services, advice, and assistance includes for the purposes of providing advice and assistance around personnel, information, and physical security, as well as advice around national security risks. Under section 14 of the ISA, NZSIS is authorised to provide advice and assistance to anyone responding to an imminent threat to the life or safety of any person in New Zealand, or any New Zealand citizen or permanent resident overseas, any person in any area that New Zealand has search and rescue responsibilities for, or any person outside the territorial jurisdiction of any country. Any information sharing undertaken by NZSIS is conducted in accordance with the DAA, as well as Ministerial Policy Statements and NZSIS policies. Disclosure of personal information by NZSIS outside New Zealand is for the purposes of IPP11(g). However should sharing disclosure outside of New Zealand occur in reliance on IPP 11(a), (c), (e), (f), (h), or (i) then IPP 12 would apply. (g) that the disclosure of the information is necessary to enable an intelligence and security agency to perform any of its functions.	
13	**Unique identifiers** *Take care when using unique identifiers*	Information drawn from CusMod and transferred into NZSIS's main intelligence analysis system will be identifiable as personal information; no unique identifiers will be generated except those required by the intelligence analysis system to function as a database	Compliant

Appendix 3: Joint Risk Management Framework

The likelihood and impact of each privacy risk have been assessed using the following measures, as per the NZIC Joint Risk Management Framework.

Table 1: Likelihood

	Likelihood	Approximate probability
Almost certain	The event is expected to occur in most circumstances History of frequent occurrence Likely to occur during the next 6 months	> 95%
Likely	The event will probably occur in most circumstances Is likely to happen/recur Likely to occur within a one year period	> 65%
Possible	The event might happen or recur occasionally May occur at least within a one to two year period	> 35%
Unlikely	Do not expect it to happen/recur although it may do so in exceptional circumstances Unlikely to occur within a one to two year period	< 35%
Rare	The event may occur in exceptional circumstances Highly unlikely to occur within the next two years No or minimal history of occurrence.	< 5%

Table 2: Risk "Consequence" Assessment Guide

	MINIMAL	MINOR	MODERATE	MAJOR	CRITICAL
Achievement of strategic priorities and goals on time and within budget, including • **delivery of products and services to customers** • **capability (people, resources, technology & tools)**	No noticeable impact on reduction of service Resources can be managed within a team without impacting on other areas	Little or no reduction in the achievement of one or more of the strategic priorities Internal customers may notice some reduction in service Resources can be managed at Branch level and may impact on other areas	Some reduction in achievement of at least one of the strategic priorities Some noticeable reduction in customer service Some resources re-directed from other activities within a Directorate and will impact on other areas of work	Non-achievement, or greatly reduced level of achievement of at least one of the strategic priorities Serious impact on ability to meet customer service levels Some FVEYs partners affected Resources redirected from within the Agency requiring significant effort and cancelling other areas of work	Total non-achievement of one or more of the strategic priorities Significant impact on customer service Significant impact on FVEYs partners Agency unable to resource action/operation, may result in Government funding being reduced/withdrawn
Health and Safety (physical and mental) of staff or contractors (where GCSB/NZSIS at fault)	Distress to the individual Injury requiring short-term first-aid care and no absence from the workplace minor impact on team	Distress to multiple people Minor injury requiring short term medical treatment and workplace absence less than one day, impacts teams across the branch	Distress to large proportion of staff Injury requiring medical treatment or lost time of 1 day to three weeks and may impact staff in multiple teams	Distress to significant number of staff and union involvement Significant lasting injury (injuries) requiring specialist medical treatment or lost time greater than three weeks impacting on staff across the directorate	Distress to staff across the NZIC Protest from union that could result in strike action Permanent disability or loss of life
Public safety due to the work we do	No increase in threat to public safety	Little or minimal increase in threat to public safety Designated terrorist entities gain ideological support from New Zealanders or New Zealand-based persons	Threat to public safety increased Designated terrorist entities gain some material support from New Zealanders or New Zealand-based persons	Threat to public safety increased significantly Designated terrorist entities gain significant material support from New Zealanders or New Zealand-based persons Loss of life or mass trauma offshore	Widespread and serious increased threat to public safety Loss of life or mass trauma in New Zealand

	MINIMAL	MINOR	MODERATE	MAJOR	CRITICAL
Security (People, physical and information)	Could cause the level of security protections to need to increase	Compromised assets or information that could lead to the need to increase security Could be expected to affect national security, government agency operations, commercial entities and /or members of the public	Deliberate breach of laws, regulations and policies that could moderately affect national security, government agency operations, commercial entities and /or members of the public	Improper use of assets or secret information resulting in some disruption and/or damage to national security, government agency operations, commercial entities and /or members of the public	Improper use of assets or secret information that could gravely compromise national security, government agency operations, commercial entities and /or members of the public
Financial /Economic /Resources	Less than $10k loss of unbudgeted expenditure	Less than $100k loss or unbudgeted expenditure	Less than $500k loss of unbudgeted expenditure Considerable economic damage directly impacting New Zealand	Less than $1m loss of unbudgeted expenditure Significant economic damage directly impacting New Zealand Significant effort needed to replace equity/capability/tangible assets	Greater than $1m loss of unbudgeted expenditure Irreversible economic damage directly impacting New Zealand Government funding reduced/ withdrawn Irretrievable loss of tangible assets
Public trust and confidence	Public concerns raised on a local basis for a limited period Local disruption for a limited period	Public concern raised on a regional basis for a prolonged period Significant disruption on a local basis for a prolonged period	Concern raised on a national basis for a limited period Significant disruption on a regional basis	Risk to public safety increased significantly	Significant and long - term life changing behaviour by persons not directly affected by the event Significant disruption for a prolonged period throughout the country

	MINIMAL	MINOR	MODERATE	MAJOR	CRITICAL
Reputational **National/ international reputation and confidence of stakeholders in our ability to deliver outcomes and commitments and manage and govern our organisation**	Embarrassment at internal stakeholder level within NZSIS No questions from the Minister Low or no media attention	Embarrassment at internal stakeholder level within NZIC Media interest is short-lived and no blame is directed at the agency	Some embarrassment to NZSIS at external agency/stakeholder level Minor impact to FVEY output Partners stop selected sharing with NZ Minister is informed and may request to be briefed Media interest is sustained for less than a week with minor criticism levelled at the agency	Major criticism Significant damage or embarrassment to NZSIS at external stakeholder level Has an impact on our FVEY partners The Government suffers reputational damage and loses confidence in the agency's senior management Requires Ministerial Briefing DG required to make a media statement Media interest is sustained for up to a week with minor criticism levelled at the agency	Irreparable damage FVEYs criticisms of NZSIS The Government suffers severe negative reputational impact, and the Prime Minister loses confidence in the Minister and/or the agency's senior management Likely to generate an independent review Media interest is sustained for a prolonged period (i.e. over a week) with major criticism levelled at the Minister and/or the agency
Operational capability (i.e. "business as usual" - BAU) **Performance of core services**	Minimal exposure of methodology Minimal impact to the functionality of the NZIC that can be managed with minimal effort	Prejudicial to the investigation or operation Minor impact to the functionality of the NZIC Threaten the efficiency or effectiveness of some aspects of programme/activity/operation(s) and may impact other business areas	Cause damage to operational effectiveness with noticeable impact on other business areas and/or minor impact to FVEY partners Critical National Infrastructure/essential service interrupted Results in significant delays of up to 6 months	Cause significant damage to op effectiveness/capability of NZIC and/or compromises FVEY capability Critical National Infrastructure/essential service/intelligence destroyed Threaten the survival or continued effective function of the programme/activity/operation Results in significant delays > 6 months	Cause exceptionally grave damage to op effectiveness within NZIC and impacts on FVEY partners Irreparable damage to the functionality of the NZIC

Table 3: Risk Rating Matrix

The residual risk rating of each CusMod privacy risk has been determined using NZIC Joint Risk Management Risk Rating Matrix below.