New Zealand Security Intelligence Service
Te Pā Whakamarumaru

NEW ZEALAND CUSTOMS SERVICE
TE MANA ĀRAI O AOTEAROA

RPT 21/155

Joint Briefing Note

Date	October 2021
To	Hon Andrew Little, Minister Responsible for NZSIS Hon Meka Whaitiri, Minister of Customs
From	s6(a) Acting Director-General of Security Christine Stevenson, Comptroller of the New Zealand Customs Service
For your	Decision

Review of CusMod direct access agreement

Purpose

1. This briefing note seeks your approval of the proposed updated Direct Access Agreement (DAA) between you as the Minister Responsible for NZSIS and the Minister of Customs ("the Ministers"), in line with section 125 of the Intelligence and Security Act 2017 ("the ISA"). The DAA is for NZSIS to have continued ongoing access to the New Zealand Customs Service ("Customs") CusMod database.

Background

2. The ISA provides for the creation of DAAs in order to enable an intelligence and security agency to directly access information held in databases maintained by certain other public authorities.

3. In 2017 the Minister Responsible for the NZSIS and the Minister of Customs entered into a DAA which gave NZSIS direct access to the CusMod database held by Customs. The CusMod database contains information on border crossing persons, goods, and craft. NZSIS's direct access to this database directly supports its ability to undertake intelligence collection and analysis, and to provide security services, advice and assistance.

4. The ISA requires DAAs to be reviewed every three years. As required, the NZSIS and Customs officials conducted a review of this agreement on their Ministers' behalf in 2020. As part of this review, officials also consulted with Privacy Commissioner (PC) and the Inspector General of Intelligence and Security (IGIS).

5. The review confirmed that the direct access provided under the DAA is of critical value to NZSIS as the DAA supports its ability to provide advice on national security risks (e.g. immigration and border security decision-making), and protective security services (e.g. security clearance assessments) in a timely fashion. It also noted that the DAA is the least intrusive means for NZSIS to obtain the information as it has already been collected by Customs and therefore access via the DAA avoids additional specific collection against an individual.

6. The review revealed that some limited updates to the DAA were worth considering. In part this is because the DAA was concluded before the ISA fully entered into force, and as such the DAA contains transitional measures which have since been superseded by the issuance of Ministerial Policy Statements and Ministerial Authorisations under the ISA.

7. The Ministers approved the review (under joint report dated 19 March 2020) on 23 March 2020 and instructed the NZSIS and Customs to initiate the process for amending the DAA, taking into account the requirements identified during the review and to consult with the IGIS and the PC on the Ministers' behalf.

8. The major changes proposed following the Ministers' review and the drafting process are:

- Making the DAA more explicit that it can be used for the creation of assumed identities for both NZSIS and GCSB (and checking related to any proposed new assumed identity);
- Removing the requirement that searching on the CusMod database only be for a 'particular entity' to allow targeted discovery; and
- Revising the Privacy Impact Assessment so that it may be classified to a lower classification level than SECRET.

ISA Requirements

9. Section 126 of the ISA states that before entering into a DAA the Ministers must be satisfied that:

a. direct access to the information is necessary to enable the intelligence and security agency to perform any of its statutory functions;
b. there are adequate safeguards to protect the privacy of individuals, including that the proposed compliance and audit requirements for the direct access, use, disclosure, and retention of the information are sufficient; and
c. the agreement will include appropriate procedures for direct access, use, disclosure, and retention of the information.

10. The details for the above factors are outlined in the DAA.

11. The Ministers must consult with the PC (s 127) and the IGIS (s 128) before entering into a DAA. The Ministers must have regard to any comments received.

12. The necessary content of a DAA is prescribed in s 129, which has been incorporated directly into the proposed CusMod DAA.

Consultation with the IGIS and Privacy Commissioner

13. The ISA requires that when drafting (or varying) a DAA, the responsible Ministers must consult with the IGIS and the PC and have regard to any comments received from them. Following the approved review in March 2020, the Ministers approved NZSIS and Customs to consult with the offices of the IGIS and PC on their behalf.

14. NZSIS and Customs are grateful for the comments and attention the IGIS and the PC (and their staff) have provided over the course of a lengthy drafting process, and for their written feedback on the proposed DAA and Privacy Impact Assessment (PIA).

15. On 1 December 2020, NZSIS facilitated delivery of the proposed DAA and PIA to the IGIS and PC for their consultation in accordance with ss 127 and 128 of the ISA.

16. On 1 February 2021, the IGIS and PC provided joint feedback. A copy of this feedback is attached at **Appendix 1** for your consideration. No fundamental concerns were raised by the IGIS or PC during these consultations, although a number of issues were raised for consideration.

17. NZSIS and Customs have amended the earlier drafts of the DAA to address the feedback from the IGIS and the PC. Most notably this has led to an unclassified version of the PIA being created to be published alongside the DAA. A Restricted level version with greater specificity will remain classified.

18. While we have not accepted all suggestions in full due to operational and technical reasons, we have taken account of the spirit of all feedback and sought to ensure this is reflected in the final agreement. NZSIS and Customs consider the proposed DAA promotes efficiencies and security while maintaining privacy safeguards for the public.

19. On 3 August 2021, NZSIS and Customs provided the IGIS and PC a joint response noting how the feedback has been incorporated and setting out two areas where clarification of the NZSIS and Customs position was needed. A copy of this response is attached at **Appendix 2** and it contains a tabled summary of the IGIS/PC comments and how they have been addressed within the proposed DAA.

20. The two areas that NZSIS and Customs sought to clarify with the IGIS and PC were:

- Firstly, that the proposed removal of the requirement that searches be conducted for a 'particular entity' is to enable target discovery, in line with the benefits of target discovery identified by the Royal Commission of Inquiry in to the terrorist attack on Christchurch masjidan. The intention is to clarify scope, necessity and proportionality.
- Secondly, to clarify that NZSIS accepts that any information held by NZSIS will be subject to the Privacy Act, but noting that in this case, Customs will be the one to make any corrections to any personal information held on the CusMod database.

21. Furthermore, a new Standard Operating Procedure was created and finalised to outline the expectations for the use and obligations for direct access agreements by NZSIS and Customs.

Next steps

22. NZSIS's General Counsel and Customs' Chief Legal Counsel - Corporate are available to brief you on the consultation to date and how we have incorporated the feedback if required.

23. If you agree with the final draft of the DAA (attached as **Appendix 3** with both the unclassified and classified PIAs), please sign the document and advise NZSIS and Customs. NZSIS will collect the signed agreement. If you wish to make any changes prior to signature, including in light of any comments received from the PC and IGIS, please advise NZSIS and Customs of the requested amendments.

24. NZSIS will work with your offices to ensure that the IGIS and PC are informed of the outcome of consultation before the DAA is made public.

25. NZSIS and Customs will ensure that the DAA, and unclassified PIA, will be published on the websites of both NZSIS and Customs in accordance with section 131 of the ISA.

Recommendations

It is recommended that you:

1	Review	The Direct Access Agreement to the Customs CusMod database.	Yes/No
2	Note	That you must have regard to the comments provided by both the Inspector-General of Security and Intelligence, and the Privacy Commissioner in Appendix One.	Yes/No
3	Approve	The Direct Access Agreement by signing the last page.	Yes/No
4	Note	NZSIS and Customs will ensure that the DAA and unclassified PIA will be published on the websites of both NZSIS and Customs in accordance with s 131 of the ISA.	Yes/No

Signed

s6(a) [redacted]

Acting Director-General of Security

Noted / Discuss

Christine Stevenson
Comptroller of the New Zealand Customs Service

Noted / Discuss

Hon Andrew Little
Minister Responsible for the NZSIS

Date: _____

Hon Meka Whaitiri
Minister of Customs

Date: _____

NOTES:

OFFICE OF THE INSPECTOR-GENERAL OF
INTELLIGENCE AND SECURITY

Privacy Commissioner
Te Mana Matapono Matatapu

1 February 2021

Rebecca Kitteridge
Director-General of Security
New Zealand Security Intelligence Service
Pipitea House
WELLINGTON

By email: s6(a) [redacted]

Rebecca Jonasson
Chief Legal Counsel - Corporate
New Zealand Customs Service
The Customhouse, 1 Hinemoa Street, Pipitea
WELLINGTON

By email: rebecca.jonassen@customs.govt.nz

Dear Director-General and Chief Legal Counsel

2020 CusMod Direct Access Agreement – consultation
IGIS ref: SI26

1. Thank you for the opportunity to provide feedback on the proposed amendments to the CusMod Direct Access Agreement ("**CusMod DAA**").

2. Our comments and questions on the proposed CusMod DAA and the Privacy Impact Assessment are set out in **Appendix One**.

3. We ask that you respond in writing to our feedback before concluding this consultation. At this stage we do not consider it necessary to meet in person to discuss our feedback. However, depending on your response a meeting may be necessary.

Yours sincerely

Brendan Horsley
Inspector-General of Intelligence and Security

John Edwards
Privacy Commissioner

P O Box 5609, Wellington 6140
enquiries@igis.govt.nz
Phone: 04 460-0030
@igisnz

Appendix One

Clause	*Comment*
1.2	As all the relevant provisions of the ISA have now commenced, reference to this can be removed and the new DAA should come into force upon signature by both parties.
2.2	The database has a name (CusMod) and for clarity and compliance with the ISA requirement that the database to be accessed must be "specified" it should be used. There is no clear reason not to use it. (See also comment below on cl 3.1.3).
3.1.3	We support the deletion of the reference to "any replacement database" for reasons previously given. The DAA and PIA cover access to the database that currently exists, and any new database would require a new DAA and PIA. If that prospect is remote and would have a long lead-in, there is no risk of sudden loss of access for NZSIS and so no need to provide for access to a replacement, nor to refer to the database in general terms that would encompass any replacement.
6.1.2 7.1.3 7.1.4	We agree that checking prospective assumed identities (for both NZSIS and GCSB) is an appropriate use of direct access to CusMod and this should be specified in the DAA.
9.3	This clause refers to an intended agreement in writing, in identical terms to the 2017 DAA. As the agreement should now exist the clause should refer to its existence and effect, rather than its future existence.
10.2.2.	A justification in relation to a national security function is so high-level it will serve no purpose. The relevant functions and purposes are already specified in clause 7 of the DAA. Clause 10 concerns the keeping of meaningful records for each particular occasion on which the database is accessed, including the justification for access in each instance. This could be indicated by wording such as "... entities sought, and the justification for the access in all the circumstances."
11.1.1.6	In the 2017 agreement this paragraph (then 11.1.1.5) noted that access 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. This has been shortened to "logged and monitored". We query why this has been done when the earlier wording is more precise and clear.
11.1.2.2	In the 2017 agreement this subclause stated the specific control that authorised NZSIS officers could only access CusMod in respect of a pre-identified entity. We see no reason to remove this. As above re cl 10.2.2, stating that a Customs record may only be transferred to NZSIS holdings if relevant to a statutory function is such a high-level requirement it will have no meaningful effect.
11.1.3.1, 11.1.3.2, 13.4	What are the relevant "international security standards for intelligence and security agencies"?
14.1	The MPS on requesting information under s 121 ISA states that consideration of the necessity of a s 121 request requires consideration of whether there is another way to obtain the information, such as a DAA. In light of that, cl 12.1 should state that NZCS information should be accessed under the DAA unless it is necessary to request it by other means (or, more specifically, under s 121).
16.2	The PIA does not require a national security classification in its entirety and could not be withheld in its entirety under the OIA. We agree that s 131 applies to the PIA, as it is in effect an annexure to the DAA (given its specification of relevant safeguards,

Clause	*Comment*
	referenced in cl 11.1). Under s 131 therefore the PIA is to be published, except if it, or provisions of it, can be withheld under the OIA. Accordingly clause 16.2 should state that the PIA will be published, except to the extent that it may be withheld under the OIA.
N/A – PIA	As noted above in comment on cl 16.2 of the DAA, and on previous occasions, the PIA does not require a national security classification in its entirety. Some paragraphs, or details in paragraphs, might merit a national security classification but the bulk of the text does not. The PSR is clear that official information must not be protectively marked to prevent or delay the release of information that does not need protection in the public interest, and over-classification is to be avoided. We suggest NZSIS paragraph mark the PIA and redact from publication any paragraphs requiring a national security classification, consistent with s 131(2)(b) ISA.
N/A - PIA	For the avoidance of doubt, we recommend that the PIA documentation should also refer to mandatory notification of privacy breaches to the Privacy Commissioner in accordance with section 114 of the Privacy Act 2020 (for instance, at page 11 under compliance and monitoring). We also note that page 10 is missing some content under "Systems Certification and Accreditation (C&A)".
N/A – PIA	Page 18 of the PIA refers to access and correction requests for CusMod information being transferred to Customs. Although this may be appropriate in some cases, there is a significance to the NZSIS holding information about a person quite apart from Customs doing so. This is particularly the case where information is extracted, copied, and transferred to the NZSIS classified network as contemplated by clause 8.1 of the direct access agreement. We consider that the NZSIS must make a case by case assessment of whether to transfer an access request to Customs and this should be reflected in the PIA.

~~RESTRICTED~~

DMS20-7-19836

New Zealand Security Intelligence Service
Te Pā Whakamarumaru

NEW ZEALAND CUSTOMS SERVICE
TE MANA ĀRAI O AOTEAROA

3rd August 2021

Brendan Horsley
Inspector-General of Intelligence and Security
By email: Brendan.horsley@igis.govt.nz

John Edwards
Privacy Commissioner
By email: enquiries@privacy.org.nz

Tēnā Kōrua

2020 CusMod Direct Access Agreement IGIS Ref: SI26

1. Thank you for your constructive feedback on our proposed draft Direct Access Agreement (**DAA**) under Part 5, subpart 2 of the Intelligence and Security Act 2017.

2. We attach a table showing our specific responses to the comments you have raised, but outline two particular responses in this letter.

Searches for 'particular entity'

3. The Report of the Royal Commission of Inquiry into the terrorist attack on Christchurch masjidan on 15 March 2019 (**RCOI**) report, which was accepted by the Government, criticises that direct access agreements have not been put in place as anticipated by Parliament. This is partially because not all DAA have been implemented.

4. Volume 3, Part 8, Chapter 9, 10 and 14 of the RCOI report discuss the benefits of target discovery, such as a deeper understanding of threats and risks, and information sharing practices. The report acknowledges that target discovery may involve analysing data collected by Public sector agencies, and that an agreement is a practical prerequisite to an effective data sharing arrangement. While not explicitly stated, findings indicated that direct access agreements could be utilised to achieve the benefits of target discovery across a larger dataset than NZSIS holds itself- whilst still being bound by normal necessity and proportionality considerations. This is also consistent with Recommendation 9(a) (made in Part 10, chapter 2), to ensure security information sharing practices enables, rather than just restricts, information sharing. [1]

5. You commented as follows on the removal of the pre-identified entity requirement: "In the 2017 agreement this sub-clause stated the specific control that authorised New Zealand Security Intelligence Service (**NZSIS**) officers could only access CusMod in respect of a pre-identified entity. We see no reason to remove this. As above re cl 10.2.2, stating that a Customs record may only be transferred to NZSIS holdings if relevant to a statutory function is such a high-level requirement it will have no meaningful effect."

6. The pre-identified entity requirement was removed because with its inclusion, the 2017 agreement does not allow for target discovery. This is relevant to NZSIS collection functions –

[1] We attach relevant excerpts from the Report concerning Target Discovery and Direct Access.

primarily to do with collection necessary to aid the identification of 'unknown, unknowns' and more usually 'known, unknowns' in line with the findings of the RCOI.

7. We note your views at paragraph 14.1 of the DAA that NZCS information should be accessed under the DAA unless it is necessary to request it by other means, to ensure it is in line with the MPS on requesting information under s121. As you know, the MPS states that consideration of the need for a s121 request requires consideration of whether there is another way to obtain the information- NZSIS and GCSB should only make a request for information where a less intrusive means of obtaining the information is not reasonably available. If unable to use the direct access agreement for this type of target discovery, NZSIS would need to rely on section 121/122 of the Intelligence and Security Act 2017 to request that information be disclosed for analysis. We do not consider that would be appropriate in a situation where there is an ability to access the information through the direct access agreement, as it will be less intrusive on the individual for NZSIS to use the DAA rather than make the request to Customs under s121.

8. If a national security incident on the scale of the Christchurch terrorist attack was to happen again, NZSIS would be expected to have utilised our available direct access agreements to the fullest extent possible.

9. The DAA will not be used to circumvent the requirements of necessity and proportionality. It will not be used for the mass collection of the CusMod database by the NZSIS, or 'fishing expeditions'. All discovery projects are first subject to pre planning and internal review and authorisation to set scope, necessity and proportionality.

10. NZSIS may receive information that partially identifies a person or group that may pose a security risk. NZSIS may have a need therefore to cross-check NZSIS holdings with information in the CusMod database. This may enable NZSIS to identify any entities that may be intending to carry out a terror attack in New Zealand. It may be that ultimately no entities can be identified that meet that criteria. However, the use of the CusMod database is a step in ensuring that no identifiable entity exists that would meet a security concern.

11. The DAA is to be used for the collection of intelligence relevant to NZSIS functions, in circumstances where we would not be able to always accurately confirm the search was being performed in respect of a 'pre-identified entity'. Below are some examples of these circumstances:

    i. there may be instances where intelligence indicates a 'known, known' person of interest may be travelling with someone from a similar group, who we assess would be likely to pose a similar concern to the 'known, known'. In that case we use information and data obtained on the 'known, known' and other indicators in an attempt to identify any other associated individuals.

    ii. Intelligence may indicate that a group of individuals with malicious intent are travelling to New Zealand. We may have numerous indicators that we can use to narrow down and hopefully identify those individuals, but this would be in circumstances where describing those individuals as 'pre-identified entities' may not be accurate.

    iii. In another situation, intelligence may indicate a particular modus operandi by an off-shore designated terrorist entity. As with the situation above we may have a number of indicators based on that organisation's activity in other States, and there is clearly a need for NZSIS to ensure, to the fullest extent possible, that a similar attack is not being planned in New Zealand.

12. In summary, we think it is a justified and appropriate change to the agreement, that is consistent with the findings of the RCOI report.

Clarification regarding application of Privacy Act to CusMod database

13. You commented that: "Page 18 of the PIA refers to access and correction requests for CusMod information being transferred to Customs. Although this may be appropriate in some cases, there is a significance to the NZSIS holding information about a person quite apart from Customs doing so. This is particularly the case where information is extracted, copied, and transferred to the NZSIS classified network as contemplated by clause 8.1 of the direct access agreement. We consider that the NZSIS must make a case by case assessment of whether to transfer an access request to Customs and this should be reflected in the PIA."

14. We agree with your comment but wish to clarify some matters:

- NZSIS does not 'hold' the CusMod database and will not be in a position to implement any requests for correction of the information on the CusMod database. Should any transferred request result in any corrections on the CusMod database, NZSIS would then seek to align any corrections to the information NZSIS holds.
- We agree that when NZSIS does 'hold' information that it has extracted from the CusMod database, it is expected that access to that information will be guided by the Privacy Act 2020.
- Any CusMod information that is brought into the main NZSIS intelligence analysis system following an investigative analysis query will be considered by NZSIS through the standard information request process.
- We have amended page 18 of the PIA therefore to confirm that the transfer and access requests that will be transferred is in relation to the information held on the CusMod database, not to information held by NZSIS.[2]

Next steps

15. We believe that other than the minor differences outlined above and in the appendix 2 that all your suggested changes have been accepted, with changes made in the draft agreement.

16. We propose to jointly brief the Ministers recommending the signing of the Direct Access Agreement. We will provide a courtesy copy of the briefing to your office in due course.

s6(a) [redacted]

General Counsel
NZSIS

s9(2)(a) [redacted]

David Soper
Chief Legal Adviso[redacted]
New Zealand Customs

[2] For your awareness there is a difference here between the APP Direct Access Agreement and CusMod.

Appendix One- Excerpts from the Royal Commission Report:

Part 8, Chapter 10:

What is target discovery?

3. When we talk about target discovery, we mean both:
   a) identifying previously unknown terrorism threats (people, groups or networks) motivated by a well-understood, known ideology; and
   b) identifying previously unknown terrorism threats (people, groups or networks) motivated by an unknown ideology – one that is not well understood. This process necessarily includes strategic intelligence assessment (including horizon scanning) to identify and better understand the new ideology.

4. Target discovery is a proactive, exploratory effort to generate and investigate leads. Investigation of these leads can help to identify previously unknown, specific subjects of interest. This helps to gain a deeper understanding of not only the threat, but also the risk. The objective is to enable Reduction and Readiness activities for that threat before it crystallises.

5. Target discovery may involve analysing data and information already collected and stored by Public sector agencies (or international partners). It may also entail sourcing new data and information. This could be through intelligence gathering online, collection of large data sets or observation of public events. The data collected can then be used to test hypotheses about existing or emerging trends.

Part 8, Chapter 9:

Information sharing must be considered in a whole of system way

59. No one Public sector agency holds all of the finished intelligence or information produced by all the Public sector agencies involved in the counter-terrorism effort. **This makes it harder to connect the dots and increases the risk that something could be missed. To ensure that there is improved information sharing among Public sector agencies and other key stakeholders, it should be considered in a whole-of-system way.**

[60. While there have been efforts to improve secure information technology, we have not seen a coordinated effort led by the Department of the Prime Minister and Cabinet and the Security and Intelligence Board to focus attention on information sharing and to overcome barriers to sharing highly classified information with all the agencies whose work would benefit from receiving it.]

Part 8, Chapter 14:

Bulk acquisition under the Act

76. **On the face of it, the direct access sharing provisions (sections 124–133) appear to contemplate bulk data acquisition.** However, the Government Communications Security Bureau uses the direct access agreements primarily to ascertain whether a person is a New Zealander. **For the New Zealand Security Intelligence Service, direct access agreements are used to obtain useful information, but not in the form of bulk data acquisition. So, in practice, the direct access agreements do not provide a mechanism for the agencies to engage in bulk acquisition.**

Direct access agreements having not been put in place as contemplated by Parliament

90. **There are considerations of principle and practicability that mean that an agreement between the relevant intelligence and security agency and the other agency is a practical prerequisite to an effective data sharing arrangement. So it is difficult to see any alternative to a structure broadly along the lines of that presently provided for in the Act.** That said, progress towards the finalisation of direct access agreements has been limited. There are currently no mechanisms to encourage other agencies to enter into such agreements.

Part 10, Chapter 2:

Public sector agencies can and should share information more widely

Recommendation 9: Direct the new national intelligence and security agency (Recommendation 2), and in the interim the Department of the Prime Minister and Cabinet, to improve intelligence and security information sharing practices, including:

> a) **driving a change in approach to the "need-to-know" principle across relevant Public sector agencies**, with special attention given to local government including the emergency management structures at the local and regional level, **to ensure it enables rather than just restricts information sharing;**
>
> **(emphasis added)**

Appendix Two

Clause	*Comment*	Draft Response
1.2	As all the relevant provisions of the ISA have now commenced, reference to this can be removed and the new DAA should come into force upon signature by both parties.	Agreed (changes made in attached CusMod agreement).
2.2	The database has a name (CusMod) and for clarity and compliance with the ISA requirement that the database to be accessed must be "specified" it should be used. There is no clear reason not to use it. (See also comment below on cl 3.1.3).	Agreed (changes made in attached CusMod agreement). Have also aligned definition of NZCS information within the definition section for consistency with APP DAA.
3.1.3	We support the deletion of the reference to "any replacement database" for reasons previously given. The DAA and PIA cover access to the database that currently exists, and any new database would require a new DAA and PIA. If that prospect is remote and would have a long lead-in, there is no risk of sudden loss of access for NZSIS and so no need to provide for access to a replacement, nor to refer to the database in general terms that would encompass any replacement.	Noted.
6.1.2 7.1.3 7.1.4	We agree that checking prospective assumed identities (for both NZSIS and GCSB) is an appropriate use of direct access to CusMod and this should be specified in the DAA.	Noted with thanks.
9.3	This clause refers to an intended agreement in writing, in identical terms to the 2017 DAA. As the agreement should now exist the clause should refer to its existence and effect, rather than its future existence.	We have amended the DAA to note a new consolidated joint SOP has been created. This SOP will be finalised before the DAA is sent to the Ministers for signing (aiming for this to be by end of July 2021).
10.2.2.	A justification in relation to a national security function is so high-level it will serve no purpose. The relevant functions and purposes are already specified in clause 7 of the DAA. Clause 10 concerns the keeping of meaningful records for each particular occasion on which the database is accessed, including the justification for access in each instance. This could be indicated by wording such as "... entities sought, and the justification for the access in all the circumstances."	Agreed (changes made in attached CusMod agreement).
11.1.1.6	In the 2017 agreement this paragraph (then 11.1.1.5) noted that access 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. This has been shortened to "logged and monitored". We query why this has been done when the earlier wording is more precise and clear.	The general safeguards have been focussed on the employee/staff usage, whereas the auditing requirements have been placed into 10.4. We believe this to be more user friendly for both relevant staff, and interested members of the public.
11.1.2.2	In the 2017 agreement this subclause stated the specific control that authorised NZSIS officers could only access CusMod in respect of a pre-identified entity. We see no	Disagreed with- for reasons given in cover letter.

	reason to remove this. As above re cl 10.2.2, stating that a Customs record may only be transferred to NZSIS holdings if relevant to a statutory function is such a high-level requirement it will have no meaningful effect.	
11.1.3.1, 11.1.3.2, 13.4	What are the relevant "international security standards for intelligence and security agencies"?	Like other Five Eyes countries, we broadly follow the US Office of the Director of National Intelligence Committee for National Security Systems Instruction 1253 and associated 'overlays' for determining the different protection levels for different systems. The network on which we maintain information we have transferred off CusMod for retention by NZSIS implements the baseline CNSS 1253 plus Intelligence Overlay A (with large parts of Intelligence Overlay B). These specify a range of additional risk-mitigation controls and go way beyond what would be required to protect the same data in CusMod. Note that while the Controls and Overlays themselves are UNCLASSIFIED, we would not be able to explain the *level* of protection we implement on our network in an UNCLASSIFIED document
14.1	The MPS on requesting information under s 121 ISA states that consideration of the necessity of a s 121 request requires consideration of whether there is another way to obtain the information, such as a DAA. In light of that, cl 12.1 should state that NZCS information should be accessed under the DAA unless it is necessary to request it by other means (or, more specifically, under s 121).	Agreed.
16.2	The PIA does not require a national security classification in its entirety and could not be withheld in its entirety under the OIA. We agree that s 131 applies to the PIA, as it is in effect an annexure to the DAA (given its specification of relevant safeguards, referenced in cl 11.1). Under s 131 therefore the PIA is to be published, except if it, or provisions of it, can be withheld under the OIA. Accordingly clause 16.2 should state that the PIA will be published, except to the extent that it may be withheld under the OIA.	Agreed and NZSIS has reviewed, consulted with Customs, and both shall publish the de-classified paragraphs of the PIA, at the same time as the Direct Access Agreement is published.
N/A – PIA	As noted above in comment on cl 16.2 of the DAA, and on previous occasions, the PIA does not require a national security classification in its entirety. Some paragraphs, or details in paragraphs, might merit a national security classification but the bulk of the text	See response above.

	does not. The PSR is clear that official information must not be protectively marked to prevent or delay the release of information that does not need protection in the public interest, and over-classification is to be avoided. We suggest NZSIS paragraph mark the PIA and redact from publication any paragraphs requiring a national security classification, consistent with s 131(2)(b) ISA.	
N/A – PIA	For the avoidance of doubt, we recommend that the PIA documentation should also refer to mandatory notification of privacy breaches to the Privacy Commissioner in accordance with section 114 of the Privacy Act 2020 (for instance, at page 11 under compliance and monitoring). We also note that page 10 is missing some content under "Systems Certification and Accreditation (C&A)".	Agreed.
N/A – PIA	Page 18 of the PIA refers to access and correction requests for CusMod information being transferred to Customs. Although this may be appropriate in some cases, there is a significance to the NZSIS holding information about a person quite apart from Customs doing so. This is particularly the case where information is extracted, copied, and transferred to the NZSIS classified network as contemplated by clause 8.1 of the direct access agreement. We consider that the NZSIS must make a case by case assessment of whether to transfer an access request to Customs and this should be reflected in the PIA.	Agreed by way of clarification in PIA (as noted in cover letter).