

~~RESTRICTED~~

01/03/2022 10:30am



New Zealand
Security Intelligence
Service
Te Pā Whakamarumaru



MINISTRY OF BUSINESS,
INNOVATION & EMPLOYMENT
HĪKINA WHAKATUTUKI

Joint Briefing Note

Date March 2022

To Hon Andrew Little, Minister Responsible for NZSIS
Hon Kris Faafoi, Minister of Immigration

From Rebecca Kitteridge, Director-General of Security
Alison McDonald, Deputy Secretary, Immigration New Zealand, Ministry of
Business, Innovation and Employment

For your Decision

Review of APP direct access agreement

Purpose

1. This briefing note seeks your approval of the proposed new Direct Access Agreement (DAA) between you as the Minister in Charge of NZSIS and the Minister of Immigration ("the Ministers"), in line with section 125 of the Intelligence and Security Act ("the ISA"). The DAA is for NZSIS to have ongoing access to Immigration NZ's Advanced Passenger Processing database (APP) and also new access to the New Zealand Electronic Travel Authority database (ETA).

Background

2. The Intelligence and Security Act 2017 (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 Immigration entered into a DAA which gave NZSIS direct access to the APP database held by MBIE. The APP database contains travel document information of passengers and crew travelling to and from New Zealand, together with craft identification and movement information. 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 MBIE conducted a review of this agreement on their Ministers' behalf.

5. The review confirmed that the direct access provided for under the DAA is of significant value to NZSIS and MBIE. For NZSIS, it allows s6(a) screening of incoming individuals assessed to be of security concern or intelligence interest when they check in for an international flight. It also supports NZSIS's ability to undertake intelligence collection and analysis by enabling searches to be conducted on previous travel to or from New Zealand. For MBIE, the DAA avoids the need to

~~RESTRICTED~~

~~RESTRICTED~~

2025.01.29.15

respond to a high volume of case-by-case requests from NZSIS for voluntary disclosure of information, and the resource implications this would entail.

6. At the same time, 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 MBIE to draft a new DAA taking into account the requirements identified during the review, as well as to expand the DAA to include access by NZSIS to the ETA database, and to consult with the Inspector General of Intelligence and Security (IGIS) and Privacy Commissioner (PC) on the Ministers' behalf.

8. The major changes proposed following the Ministers' review and the drafting process are:
- a. Updating the DAA to better describe the circumstances in which APP information may be disclosed by NZSIS to another agency (whether in New Zealand or overseas);
 - b. Updating the audit provisions to better reflect how audits of NZSIS's access to APP information work in practice;
 - c. Updating the DAA and PIA to better reflect how information requests related to the databases will be handled; and
 - d. To include access to the ETA database within the DAA.

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 Ministers must consult with, and invite comment from, the PC and the IGIS before entering into a proposed DAA or proposed agreement to vary a DAA (ss 127, 128, 130). The Ministers must have regard to any comments received on the proposed agreement.

11. The necessary content of a DAA is prescribed in s 129, which has been incorporated directly into the proposed APP and ETA DAA.

Consultation with the IGIS and Privacy Commissioner

12. The Ministers instructed NZSIS and MBIE to conduct the statutory consultation with the IGIS and PC on their behalf. On 8 December 2020, NZSIS facilitated delivery of the proposed DAA and PIA to the IGIS and PC for their consultation.

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

~~RESTRICTED~~

~~RESTRICTED~~

CONFIDENTIAL

14. On 28 January 2021 the IGIS and PC provided joint feedback. A copy of this feedback is attached at **Appendix 1**. No fundamental concerns were raised by the IGIS or PC during these consultations, although a number of issues were raised for consideration.

15. NZSIS and MBIE 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 PIAs being created to be published alongside the DAA. Restricted level versions with greater specificity will remain classified.

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

17. On 26 July 2021 NZSIS and MBIE provided the IGIS and PC a joint response noting out how the feedback has been incorporated and setting out one particular area where clarification of the NZSIS and MBIE 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 effected into the proposed DAA.

18. The one particular area that NZSIS and MBIE sought to clarify with the IGIS and PC is the way in which requests for information regarding information on the APP database would be processed. The way in which APP has been operationalised is different from other DAAs. INZ pushes its database and any updates to it through to a locked down system in NZSIS's information infrastructure, rather than how access to the Customs database works where a Customs controlled terminal is held within an NZSIS location.

19. Technically therefore the APP database is 'held' by NZSIS as well as by INZ, although the information is locked down to only authorised users who may only access APP database for authorised purposes.

20. Both NZSIS and MBIE's view is that any information that is only held on the APP database should only be accessed by NZSIS for purposes authorised under the DAA, and that NZSIS searching APP only in relation to a Privacy Act request would be more appropriately handled through transferring the request to MBIE as allowed under section 43(1)(b) of the Privacy Act.

21. Any data that has been brought from the APP database into NZSIS's intelligence holdings will be subject to the usual information request considerations under the Privacy Act and Official Information Act.

22. On 13 October 2021 a further letter was received from the IGIS and PC on this point suggesting a pragmatic solution to how NZSIS should respond to requests for such information (and some other incidental suggestions). These have been accepted by the agencies and changes implemented as noted in our 13 December response. A copy of the IGIS and PC letter and the joint response is attached at **Appendix 3**.

Next steps

23. NZSIS's General Counsel and MBIE's General Manager, Data, Insights and Intelligence are available to brief you on the consultation to date and how we have incorporated the feedback.

24. If you agree with the final draft of the DAA (attached as **Appendix 4**), please sign the document and advise NZSIS and MBIE. NZSIS will collect the signed agreement. If you wish to make

~~RESTRICTED~~

~~RESTRICTED~~

any changes prior to signature, including in light of any comments received from the PC and IGIS, please advise NZSIS and MBIE of the requested amendments.

25. NZSIS will inform the IGIS and PC of the below recommendations before the DAA is made public.

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

Recommendations

It is recommended that you:

- | | | | |
|---|---------|--|--------|
| 1 | Review | The Direct Access Agreement to the MBIE APP and ETA databases. | 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 and Three. | Yes/No |
| 3 | Approve | The Direct Access Agreement by signing the last page. | Yes/No |
| 4 | Note | NZSIS and MBIE will ensure that the DAA and unclassified PIAs will be published on the websites of both NZSIS and MBIE in accordance with s 131 of the ISA. | Yes/No |



Rebecca Kitteridge
Director-General of Security



Alison McDonald
Deputy Secretary Immigration,
Immigration New Zealand
Ministry of Business, Innovation and
Employment

Noted / Discuss

Noted / Discuss

Hon Andrew Little
Minister Responsible for NZSIS

Hon Michael Wood
Minister of Immigration

Date: _____

Date: _____

~~RESTRICTED~~

~~RESTRICTED~~

CONFIDENTIAL

NOTES:

~~RESTRICTED~~

Released under the Official Information Act 1982

1



OFFICE OF THE INSPECTOR-GENERAL OF
INTELLIGENCE AND SECURITY

28 January 2021

Rebecca Kitteridge
Director-General of Security
New Zealand Security Intelligence Service
Pipitea House
WELLINGTON
By email: **s6(a)**

Greg Patchell
Deputy Chief Executive, Immigration
Ministry of Business, Innovation and Employment
Stout Street
WELLINGTON
By email: greg.patchell@mbie.govt.nz

Dear Director-General and Mr Patchell

2020 APP and ETA DAA Review – consultation

1. Thank you for the opportunity to provide feedback on the proposed amendments to the Advance Passenger Processing and Electronic Travel Authority Direct Access Agreement (“**APP and ETA DAA**”).
2. Our comments and questions on the proposed APP and ETA DAA are set out in **Appendix One**.
3. We request the NZSIS and the MBIE respond in writing to our feedback prior to concluding this consultation. At this stage, we do not consider it necessary to meet in person to discuss our feedback. However, depending upon the response of both the NZSIS and MBIE, a meeting may be necessary.

Yours sincerely

Brendan Horsley
Inspector-General of Intelligence and Security

John Edwards
Privacy Commissioner

Appendix One

<i>Clause</i>	<i>Comment</i>
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.
3.1	Include the definitions of "APP information" (cl 5.1) and "ETA information" (cl 5.2) to make the document easier to read as a whole.
8.1	The Service will hold a copy of the DAA information on its fully accredited system. Given this statement, it would be appropriate for the Service to respond to Privacy Act requests by referencing the APP data it holds on a person. There is a significance to the NZSIS holding information about a person quite apart from MBIE doing so. Any transfers of Privacy Act requests to MBIE must be lawfully made in accordance with section 43 of the Privacy Act 2020.
10.1	The Service should harmonise its approach to audits under the APP and ETA DAA with the CUSMOD DAA (cl 10.4) and the BDM DAA (cl 10.4). The new version of the APP DAA imposes a more flexible requirement.
11.2.5	Inappropriate access by Service employees to APP and ETA information is a significant risk. Security and compliance auditing should be routine (and ad hoc where necessary in specific circumstances).
11.3.1	We consider the DAA should also require the system on which information is to be held to be "fully accredited at all times". Ensuring the system is at all times fully accredited is an important mechanism to protect this personal information.
11.3.1, 13.4	What are the international security standards for intelligence and security agencies?
11.3.6	In practice how would the Service access information about juveniles if that information is normally filtered out? Must a special request be made of MBIE to release that information?
11.3.8	Does the Service have the capability to label data in the way this clause envisages?
12.2	During a previous consultation, the Service indicated it did not have enough data available to assess whether a 10-year retention period was appropriate or not. We suggest the DAA include a date by which a review of the retention period needs to take place in order to assess whether the retention period is necessary and proportionate to the use of the information by the NZSIS.
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 MBIE 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, 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	For the avoidance of doubt, we recommend that documentation should also refer to mandatory notification of privacy breaches to the Privacy Commissioner in accordance with section 114 of the Privacy Act 2020.



New Zealand
Security Intelligence
Service
Te Pā Whakamarumarū



MINISTRY OF BUSINESS,
INNOVATION & EMPLOYMENT
HĪKINA WHAKATUTUKI

23 July 2021

Brendan Horsley
Inspector-General of Intelligence and
Security

By
Brendan.horsley@iqis.govt.nz

email:

John Edwards
Privacy Commissioner

By email: enquiries@privacy.org.nz

Dear Sirs

2020 APP and ETA Direct Access Agreement

1. Thank you for your constructive feedback on our proposed draft direct access agreement.
2. We attach a table showing our specific responses to the comments you have raised, but outline one particular response in this letter.

Clarification regarding application of Privacy Act to APP and ETA database

Your comment:

"The Service will hold a copy of the DAA information on its fully accredited system. Given this statement, it would be appropriate for the Service to respond to Privacy Act requests by referencing the APP data it holds on a person. There is a significance to the NZSIS holding information about a person quite apart from MBIE doing so. Any transfers of Privacy Act requests to MBIE must be lawfully made in accordance with section 43 of the Privacy Act 2020."

3. We are not suggesting that any APP information that NZSIS have brought into their holdings in the performance of their functions would not be subject to requests to NZSIS and have made that clear in clause 12.3 of the DAA.
4. While we believe it is technically correct that we 'hold' APP information by virtue of that being the way that MBIE has facilitated direct access in this case, all of the information made available by MBIE under the DAA is not 'held' within NZSIS regular holdings. The relationship between MBIE and NZSIS prior to information being brought into NZSIS holdings is most akin to that of an agent for safe custody – pending the information actually being directly accessed by the NZSIS for the performance of the functions outlined in the DAA.
5. We respectfully submit that the significance attributed to the fact that we hold APP data apart from MBIE is inaccurate in a practical sense and we are therefore reluctant to amend clause 7 of the DAA to allow us to review APP information

Property of the New Zealand Security Intelligence
Service. Reclassification, or dissemination requires
prior consent.

outside of the performance of our ISA functions. To hold otherwise could lead to the unintended consequence of unnecessary access to the information by reason of receipt of a Privacy Act request and our need to then search the APP database for that requestor's details, when we do not otherwise hold any records concerning that person. If the requestor's details are within the APP database, we would then have to bring the data back into our system and respond that we do hold information about them (or NCND), giving rise to a potential concern for the requestor when one should not exist.

6. Rather, in circumstances where NZSIS have not brought that information into NZSIS' intelligence holdings, NZSIS are only holding the copy of the APP database for access in limited specified circumstances. In that way, NZSIS is holding the data to potentially enable a form of access only, most akin to holding as an agent of MBIE, without knowing what it holds. In those circumstances MBIE is the most appropriate agency to respond to any Privacy Act request received by NZSIS relating to information held that may encompass APP data, as the request relates to functions and activities more closely connected with MBIE as allowed under section 43(1)(b) of the Privacy Act 2020.
7. We believe the ability to transfer under section 43(1)(b) of the Privacy Act 2020 is available in this case, and that it would be an improper purpose of the DAA to only access the APP (or ETA) database for the sole purpose of responding to an IPP access request, when NZSIS believe that the information to which the request relates is more closely connected with the functions or activities of MBIE.
8. As noted above, if NZSIS are unable to transfer requests in such a way the alternative will be that any individual requester will have to have their APP information brought within our intelligence holdings, in circumstances where it is unlikely they would ever have had their personal information on our files before, which we do not consider to be an appropriate use of the DAA.

Next steps

9. We believe that other than the minor differences outlined above and in the attached table that all your suggested changes have been accepted, with changes made in the draft agreement.
10. We are happy to meet to discuss the above point if that would further assist. Alternatively, if it is accepted that a transfer of such IPP requests to MBIE is the appropriate approach we will proceed to jointly brief the Ministers, and recommend signature of the Direct Access Agreement. We will provide a courtesy copy of the briefing in case there is anything further you wish to raise with the Ministers directly.

s6(a)

General Counsel
NZSIS

s9(2)(a)

Catriona Robinson
Deputy Secretary, Immigration (Acting)
MBIE

Appendix One- Comments Table

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 draft).
3.1	Include the definitions of "APP information" (cl 5.1) and "ETA information" (cl 5.2) to make the document easier to read as a whole.	Agreed (changes made in attached draft).
8.1	The Service will hold a copy of the DAA information on its fully accredited system. Given this statement, it would be appropriate for the Service to respond to Privacy Act requests by referencing the APP data it holds on a person. There is a significance to the NZSIS holding information about a person quite apart from MBIE doing so. Any transfers of Privacy Act requests to MBIE must be lawfully made in accordance with section 43 of the Privacy Act 2020.	Explained in cover letter.
10.1	The Service should harmonise its approach to audits under the APP and ETA DAA with the CUSMOD DAA (cl 10.4) and the BDM DAA (cl 10.4). The new version of the APP DAA imposes a more flexible requirement.	For similar reasons to 8.1 above and that the nature of how we access the APP database is different from BDM and Cusmod access and that therefore a 'joint audit' is not really possible as NZSIS are not accessing an MBIE held database that they can monitor, rather as noted in your comments to 8.1, the APP database is actually held by NZSIS. MBIE have the ability to review our audit if required through a suitably cleared employee as per 10.1.
11.2.5	Inappropriate access by Service employees to APP and ETA information is a significant risk. Security and compliance auditing should be routine (and ad hoc where necessary in specific circumstances).	Agreed – have left the more general 'ad hoc' requirement in without reference to the specific circumstances to allow greater flexibility for audit.
11.3.1	We consider the DAA should also require the system on which information is to be held to be "fully accredited at all times". Ensuring the system is at all times fully accredited is an important mechanism to protect this personal information.	8.1 already states the information will be held on a fully accredited system- have added 'accredited' to 11.3.1 to remove doubt.
11.3.1, 13.4	What are the 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 the s6(a) system that houses APP (and will house ETA) data implements

~~RESTRICTED~~

		<p>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 this data in MBIE systems. Broadly speaking, we are applying controls suitable for TOP SECRET COMINT information to IN CONFIDENCE personal data.</p> <p>Note that while the Controls and Overlays themselves are UNCLASSIFIED, we would not be able to explain the <i>level</i> of protection we implement on our network in an UNCLASSIFIED document.</p>
11.3.6	In practice how would the Service access information about juveniles if that information is normally filtered out? Must a special request be made of MBIE to release that information?	The default search filters out juveniles. Should a specific need arise to search for information about children then our usual SCI policies would apply and therefore the appropriate approval level for lead investigation or otherwise would flow from the SCI JPS. If approval was given, then the search query could be altered to include juveniles within the scope of the approval.
11.3.8	Does the Service have the capability to label data in the way this clause envisages?	Yes. s6(a) <div style="background-color: black; color: white; padding: 2px;">50</div> anything brought from APP into s6(a) (both from alerts or from a specific query) has the value "APP" applied. The same process will be used for ETA information.
12.2	During a previous consultation, the Service indicated it did not have enough data available to assess whether a 10-year retention period was appropriate or not. We suggest the DAA include a date by which a review of the retention period needs to take place in order to assess whether the retention period is necessary and proportionate to the use of the information by the NZSIS.	There has not been enough usage to conduct a meaningful review of whether the 10 year retention period is appropriate or not. The oldest data we current have is from September 2011. We have put in a requirement at clause 12.3 to complete a review over the course of this intended 3 year DAA to inform the next review.
14.1	The MPS on requesting information under s 121 ISA states that consideration of the necessity of an 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 MBIE information should be accessed under the DAA unless it is necessary to request it by other means (or, more specifically, under s 121).	In general we agree with this principle and have made changes to the draft at clause 14.1. We note that this will only apply to APP and ETA information and not all MBIE information. We want to retain the ability to make 121 requests when systems are down or we don't have enough CusMod users etc.

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.
N/A – PIA	For the avoidance of doubt, we recommend that documentation should also refer to mandatory notification of privacy breaches to the Privacy Commissioner in accordance with section 114 of the Privacy Act 2020.	Agreed.



OFFICE OF THE INSPECTOR-GENERAL
OF INTELLIGENCE AND SECURITY

13 October 2021

General Counsel
New Zealand Intelligence Service
Pipitea House
Pipitea Street
WELLINGTON
By email: **s6(a)**

Catriona Robinson
Deputy Secretary, Immigration (Acting)
Ministry of Business, Innovation and Employment
Stout Street
WELLINGTON
By email: catriona.robinson@mbie.govt.nz

Dear Counsel and Ms Robinson

1. Thank you again for the agencies' engaged response of 23 July 2021 and agreement to make the majority of the proposed changes to the DAA. Our apologies for the delay in further communications. We have now had an opportunity to consider the draft DAA (23 July 2021 version) and have several further comments. These predominantly concern how the Service might best approach the APP and ETA information/data it holds when responding to requests under the Privacy Act 2020 (PA). Following that, we have several comments on more incidental matters.

An approach to APP and ETA data in response to Privacy Act requests

Clauses 7, 8.1 and 12.3

2. The PA (and the OIA) do not distinguish between the sorts of repositories or systems in which an agency, subject to those Acts, "holds" personal (and/or official) information. It follows that it is immaterial to requests made under the PA whether the Service holds the APP and ETA data in a specific or a "regular" location in its accredited systems, or whether it considers the holding to be akin to a form of "safe custody". Clause 12(3) of the DAA therefore seeks to impose limits which are unavailable to the Service in law (ie, limits related to which information held by the Service is subject to the PA and/or OIA).
3. As we indicated in our letter of 28 January 2021, in effect the Service holds a copy of the APP and ETA information, to carry out the broadly described statutory functions under ISA, as set out at clause 7 of the DAA, although we appreciate that in practice the Service places limits on in-house access and on search mechanisms.

Released under the Official Information Act 1982

4. We would not accept the suggestion, at paragraphs 6 and 7 of your letter, that a transfer of a PA request to MBIE is appropriate with regard to APP and ETA information. If this was adopted as the Service's approach, it would then have to transfer every PA request it received to MBIE, in case the requestor appeared in the APP and ETA databases. You note at paragraph 5 a preference to avoid causing potential concern to a requestor. We believe this concern (and we would add, confusion) would be significantly increased by a requestor receiving a letter from the NZSIS saying the individual's request for any personal information held by the Service was being transferred to MBIE. In our view, it is something of a stretch to consider such a PA request to the Service as being more closely connected with the functions of MBIE.
5. Nonetheless, we are also mindful that both the Privacy Commissioner and the Chief Ombudsman have on occasion clarified that there is no requirement for agencies to create or develop new information in order to respond to requests under those Acts. This consideration may – to a very limited extent – have some relevance to the Service's APP and ETA holdings when the Service processes PA requests.
6. We suggest there is an alternative way in which the Service might approach PA requests with regard to the APP and ETA information it holds. The Service may wish to develop a standard paragraph for inclusion in all its responses to PA requests, which states something along the following lines:
 - a. The Service holds a copy of MBIE's APP and ETA databases within the Service's systems (as per Schedule 2 of ISA);
 - b. What this APP and ETA data contains and how the Service accesses this information in set out in the DAA and PIA [along with where the DAA and PIA may be found online];
 - c. If the requestor has travelled to or from New Zealand within the past ten years, then the requestor should be aware that their personal information will be recorded in those databases (given that is the primary purpose of those databases);
 - d. Either of the following sentences, as appropriate: The Service has not conducted a search of the APP and ETA databases for the purposes of the person's PA request; Or The Service can neither confirm nor deny whether it has conducted a search of the APP and ETA databases for the purposes of the person's PA request;¹
 - e. The person will be aware of whether or not their travels will have resulted in their data being recorded in the APP and ETA databases. If the person has any concerns about that, they should contact MBIE [and provide contact details].
7. To accompany this approach, we are also seeking the addition of a sentence to clause 8.1, as follows: "This copy will be held separately from NZSIS' intelligence holdings, in a segregated database and is held solely to enable NZSIS' direct access to APP and ETA information under this Agreement."
8. If the approach is accepted by the Service (and MBIE), the Commissioner and Inspector-General would seek to review the draft paragraph as outlined above, and the necessary related changes

¹ The Service will have to make a case by case assessment when responding to PA requests, as to which form of sentence is appropriate.

made to the DAA. We suggest that the Service also includes a generic paragraph to this effect on the NZSIS webpage about Privacy Act requests.

Incidental matters

Clauses 11.3.1 and 13.4 International standards

9. We appreciate the information provided about the relevant “international security standards for intelligence and security agencies” as referenced in these two clauses. For clarity and as this material is publicly available (at high level), we suggest this term be included in the definitions at clause 3 of the DAA, as corresponding to “US Committee for National Security Systems Instruction 1253”.

Clause 12.2 Retention timeframe

10. We note the useful addition of the requirement in clause 12.2 for the Service to carry out an interim review of the ten year retention period, prior to the next Ministerial review of the DAA in 2024. As you know, we remain interested in whether the ten year period is necessary and appropriate. But we do no more at this stage than flag we will be keen to see robust justifications/examples for that timeframe or similar, if the agencies intend it to remain in place in the future.

Clause 13.2 Countries/states as the subjects of Ministerial authorisations

11. At clause 13.2 the DAA records that these authorisations are classified, and so paraphrases them at 13.2.1 to 13.2.3. While we agree the specific detail of each of these authorisations has not been made public, the fact that they mostly concern countries/states rather than “specified persons” (13.2.3) is already in the public domain. For example, in the consideration of Ministerial authorisations, included in the Inspector-General’s 2019 Public Report *Inquiry into possible New Zealand intelligence and security agencies’ engagement with the CIA detention and interrogation programme 2001-2009*, it was stated that there were “two broad standing Ministerial authorisations covering a large number of states”.² We therefore suggest clause 13.2.3 of the DAA be amended to record something along the lines of: “other specified countries”.

12. We look forward to your response on our above comments and suggestions.

Yours sincerely



Brendan Horsley
Inspector-General of Intelligence and Security



John Edwards
Privacy Commissioner

Copy to: s6(a) NZSIS Legal Team s6(a)

² This wording can be found in the IGIS Public Report at [268], with similar wording repeated at, for example, [273], [274] and [277].

~~IN CONFIDENCE~~



New Zealand
Security Intelligence
Service
Te Pā Whakamarumaru



**MINISTRY OF BUSINESS,
INNOVATION & EMPLOYMENT**
HĪKINA WHAKATUTUKI

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

Dear Sirs

APP and ETA Direct Access Agreement

1. Thank you for your letter dated 13 October 2021 providing further comments on our proposed draft direct access agreement.
2. Your letter highlighted two particular areas, one related to a suggested response by the NZSIS to Privacy Act requests in relation to the APP and ETA databases, the other related to some minor comments on incidental matters related to the drafting.
3. We provide responses to each of the above in turn.

Suggested approach to APP and ETA Data in response to Privacy Act requests

4. We note your concerns around the propriety of transfer by NZSIS to MBIE of information requests regarding information on the APP and ETA databases that has not been accessed by the NZSIS and brought into its main intelligence holdings.
5. We appreciate your suggested process to address these concerns, which provides transparency as to NZSIS holdings, without creating a need to review irrelevant (in relation to ISA functions) information regarding individuals. We therefore accept your suggested approach, and have also amended clause 8.1 as proposed.
6. You have requested to review the standard paragraph NZSIS proposes to include in response to all Privacy Act requests. We attach this as Appendix One, along with the proposed text for NZSIS's website.

~~IN CONFIDENCE~~

~~IN CONFIDENCE~~

Incidental matters

7. In short we accept all of your proposed incidental amendments outlined in paragraphs [9] and [11] of your 13 October 2021 letter. We outline those changes in the attached table at Appendix Two.

Next steps

8. If you have any further comment on NZSIS's proposed response for Privacy Act requests, we ask that these be provided by close of **22 December**. This will enable us to proceed with briefing our Ministers on the DAA and consultation process, with a view to, subject to Ministerial approvals, executing and publishing the DAA prior to Christmas.
9. We will provide a courtesy copy of the finalised joint briefing in case there is anything further you wish to raise with the Ministers directly.
- 10 Many thanks for your constructive comments throughout the consultation process for the amended DAA. We appreciate this has been a lengthy process, given the various competing priorities and Covid related difficulties we have all faced over these last 18 months, and very much appreciate your continued engagement and attention throughout

s6(a)

General Counsel
NZSIS



Alison McDonald
Deputy Secretary, Immigration
MBIE

~~IN CONFIDENCE~~

~~IN CONFIDENCE~~

Appendix One-

Standard text for responses:

Please note that the NZSIS holds copies of Ministry of Business and Employment's Advanced Passenger Processing and Electronic Travel Authority databases. More detail on this can be found in our Direct Access Agreement and Privacy Impact Assessments which are available on our website at [insert link].

[The NZSIS has not conducted a search of these records for the purposes of responding to your Privacy Act request.]

OR

[The NZSIS can neither confirm nor deny whether it has conducted a search of these databases for the purposes of your Privacy Act request.]

If you have travelled to or from New Zealand within the last ten years, there will be personal information about your travel in these records. If you have any questions about this information, you can contact MBIE at [MBIE contact details].

Text for website:

The NZSIS holds copies of Ministry of Business and Employment's Advanced Passenger Processing and Electronic Travel Authority databases. More detail about these records and our access can be found in the below documents:

[Link to direct access agreement]

[Link to PIA for APP]

[Link to PIA for ETA]

We do not search these databases when responding to Privacy Act requests. If you have travelled to or from New Zealand in the past ten years there will be personal information about your travel in these records. If you have any questions about this information, you can contact MBIE [link to MBIE website]

~~IN CONFIDENCE~~

~~IN CONFIDENCE~~

Appendix Two- Comments Table

Clause	IGIS/OPC Comment	Draft Response
6	<p>The Service may wish to develop a standard paragraph for inclusion in all its responses to PA requests, which states something along the following lines:</p> <p>a. The Service holds a copy of MBIE's APP and ETA databases within the Service's systems (as per Schedule 2 of ISA);</p> <p>b. What this APP and ETA data contains and how the Service accesses this information is set out in the DAA and PIA (along with where the DAA and PIA may be found online);</p> <p>c. If the requestor has travelled to or from New Zealand within the past ten years, then the requestor should be aware that their personal information will be recorded in those databases (given that is the primary purpose of those databases);</p> <p>d. Either of the following sentences, as appropriate: The Service has not conducted a search of the APP and ETA databases for the purposes of the person's PA request; Or The Service can neither confirm nor deny whether it has conducted a search of the APP and ETA databases for the purposes of the person's PA request;¹</p> <p>e. The person will be aware of whether or not their travels will have resulted in their data being recorded in the APP and ETA databases. If the person has any concerns about that, they should contact MBIE (and provide contact details).</p>	Agreed – draft standard paragraph attached at Appendix Two.
8.1	<p>To accompany this approach, we are also seeking the addition of a sentence to clause 8.1, as follows:</p> <p>"This copy will be held separately from NZSIS' intelligence holdings, in a segregated database and is held solely to enable NZSIS' direct access to APP and ETA information under this Agreement."</p>	Agreed- changes made to our finalised DAA, and will update the Privacy request information on our website with a generic paragraph as indicated in Appendix Two, outlining the approach at the same time as the new DAA is published.
11.3.1 and 13.4	For clarity and as this material is publicly available (at high level), we suggest this term be included in the definitions at clause 3 of the DAA, as corresponding to "US Committee for National Security Systems Instruction 1253".	Agreed – changes made.
13.2	We therefore suggest clause 13.2.3 of the DAA be amended to record something along the lines of: "other specified countries".	Agreed – changes made to include countries. We have changed to "countries or authorised persons" in order to more accurately reflect the scope of the authorisation.

~~IN CONFIDENCE~~



New Zealand
Security Intelligence
Service
Te Pā Whakamarumaru



Te Tari Taiwhenua
Internal Affairs

Direct access to DIA Information by NZSIS

Date September 2022

To Hon Andrew Little, Minister Responsible for NZSIS
Hon Jan Tinetti, Minister of Internal Affairs

From Rebecca Kitteridge, Director-General of Security
Paul James, Secretary for Internal Affairs

For your Decision

Seeking approval of direct access agreement to Department of Internal Affairs Information by NZSIS

Purpose

1. This briefing note seeks your approval for the proposed new Direct Access Agreement (**DAA**) between you as the Minister in Charge of NZSIS and the Minister of Internal Affairs (**the Ministers**), in line with section 125 of the Intelligence and Security Act (**the ISA**). The DAA is for NZSIS to continue having ongoing access to the Registrar-General of Births, Deaths and Marriages Registration information database (**BDMI database**), as well as providing new ongoing access to the Secretary for Internal Affairs' Citizenship information database (**Citizenship Database**). For ease of reference we refer to the BDMI database and the Citizenship database as **DIA information**.

Background

2. The Intelligence and Security Act 2017 (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 2018 the Minister Responsible for the NZSIS and the Minister of Internal Affairs entered into a DAA which gave NZSIS direct access to the BDMI database held by the Registrar-General within the Department of Internal Affairs.
4. 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. It also supports the acquisition, use and maintenance of assumed identities under the ISA.
5. The ISA requires DAAs to be reviewed every three years. As required by section 132 of the ISA, a review of this agreement was conducted, and the Inspector-General of Intelligence and Security (**IGIS**) and the Privacy Commissioner (**PC**), were consulted on that review.

6. The review confirmed that the direct access provided for under the existing DAA is of significant value to NZSIS but was unable to be operationalised as previously envisaged. The particular aspect that caused the most difficulty is the existing DAAs prohibition on access to the information from within NZSIS facilities. This created both operational security risks as well as further complications given the restricted ability for staff to move between Government buildings in the current Covid environment.

7. The review also recommended that addition of the Citizenship database within the DAA as well as a number of other changes to better align the DAA with the wording used in other direct access agreements.

8. Under briefing note dated 1 December 2021 the Ministers approved the recommendations and proposed:

- a. To incorporate the Citizenship Database within the DAA;
- b. To amend the DAA to allow access to DIA information from within NZSIS facilities;
- c. To align the audit and authorisation safeguards as much as possible with those outlined in the DAA with the Minister of Customs;
- d. To align the wording with other current DAAs (such as those with the Minister of Customs, and Minister of Immigration), and to confirm that DAA may be used for the purpose of target discovery, and also that NZSIS may access for the purpose of checking assumed identities on behalf of GCSB.

9. The Ministers also directed NZSIS and DIA to again consult with the PC and IGIS on their behalf as required by sections 127 and 128 of the ISA.

ISA Requirements

10. 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
the agreement will include appropriate procedures for direct access, use, disclosure, and retention of the information.

11. As noted above 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 DAA.

Consultation with the IGIS and Privacy Commissioner

13. NZSIS and DIA are grateful for the comments and attention the IGIS and the PC (and their staff) have provided over the drafting process, and for their written feedback on the proposed DAA and Privacy Impact Assessment (PIA).

14. On 13 December 2021, NZSIS provided the proposed DAA and PIA to the IGIS and PC for their consultation in accordance with ss 127 and 128 of the ISA.
15. On 28 January 2022 the office of the IGIS provided feedback. A copy of this feedback is attached at **Appendix 1**.
16. On 31 January 2022 the office of the acting PC provided feedback. A copy of this feedback is attached at **Appendix 2**.
17. No fundamental concerns were raised by the IGIS or PC during these consultations, although a number of issues were raised for consideration.
18. NZSIS and DIA have amended the earlier drafts of the DAA to address the feedback from the IGIS and the PC, and incorporated all their suggestions.
19. On 8 June 2022 NZSIS and DIA provided the IGIS and PC a joint response noting out how the feedback has been incorporated. There were no particular outstanding matters that required detailed explanation in our response but we did provide some high-level information around NZSIS's approach to the Crown Maori Relationship and ongoing work being implemented to develop and mature the NZSIS's understanding of how the Crown Maori Relationship impacts our work.
20. A copy of this response is attached at **Appendix 3** and it contains a tabled summary of the IGIS/PC comments and how they have been placed into the proposed DAA. Although, it was not anticipated as we had incorporated all comments received, any final comments were invited to be received by 30 June.
21. Both IGIS and PC have advised they have no further comments to make.

Next steps

22. NZSIS's General Counsel and DIA's Chief Legal Adviser are available to brief you on the consultation to date and how we have incorporated the feedback.
23. There has been a minor change to the Privacy Impact Assessment to better describe the description of the Virtual Private Network in Risk 1 on page 10 that both agencies consider would not impact on the oversight comments above.
24. NZSIS and DIA attach for your consideration the Privacy Impact Assessment (**Appendix 4**) and final draft of the DAA (**Appendix 5**). If you agree with the final draft of the DAA, please sign the document and advise NZSIS and DIA. 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 DIA of the requested amendments.
25. 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.
26. NZSIS and DIA will ensure that the DAA, and unclassified PIA, will be published on the websites of both NZSIS and DIA in accordance with section 131 of the ISA.

~~RESTRICTED~~

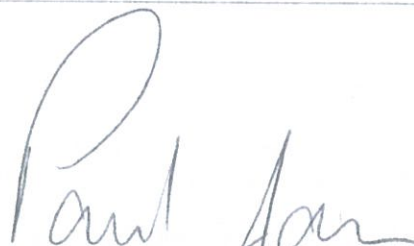
Recommendations

It is recommended that you:

			Minister for NZSIS	Minister of IA
1	Review	The Direct Access Agreement to DIA information	Yes / No	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 Appendices 1 and 2.	Yes / No	Yes / No
3	Note	The Privacy Impact Assessment (attached at Appendix 4).	Yes / No	Yes / No
4	Approve	The Direct Access Agreement (attached as Appendix 5) by signing the last page.	Yes / No	Yes / No
5	Note	NZSIS and DIA will ensure that the DAA and PIA will be published on the websites of both NZSIS and DIA in accordance with s 131 of the ISA.	Yes / No	Yes / No



Rebecca Kitteridge
Director-General of Security
New Zealand Security Intelligence Service



Paul James
Secretary for Internal Affairs
Department of Internal Affairs

Hon Andrew Little
Minister Responsible for
New Zealand Security Intelligence Service

Hon Jan Tinetti
Minister of Internal Affairs

~~RESTRICTED~~

Feedback from IGIS on the draft Direct Access Agreement (DAA) between the Department of Internal Affairs and the New Zealand Security Intelligence Service

- **9.2.1 and 9.2.2 (pg. 5):** Can we please confirm if this is a one-time only training or annual training?
- **9.3 (pg. 6):** Can we please be provided with a copy of the Joint SOP?
- **9.4, 10.2 and 10.3 (pg. 6):** For oversight purposes, the IGIS should have access to this record.
- **10.4 (pg. 6):** For oversight purposes, we recommend that, if there is any significant delay in the yearly audit of this DAA, the IGIS is notified of the delay.
- **13.5 (pg. 8):** What guidance is there for NZSIS staff when considering the Crown relationship with Maori under the Treaty of Waitangi?
- **13.6 (pg. 8-9):** We recommend that this section should reference the relevant Ministerial Policy Statements (i.e. cooperation with overseas public authorities).

Feedback from IGIS on the draft Privacy Impact Assessment (PIA)

- **13 (iii) (pg. 5):** We note that this is not a statutory function of the NZSIS, and the statutory functions refer to s 10 and 11 ISA.
- **16 (pg. 5):** will there be a SOP regarding discovery activities conducted by the Service under this DAA?
- **25 (pg. 6):** We believe that this is a typo and the word should be “international”.
- **Footnote 7 (pg. 6):** According to the ISA, the NZSIS does not have “information assurance and cybersecurity services” functions, and these are the function of the GCSB (s 12). And for ease of use, we also suggest the references in the footnote are linked to the relevant sections in the ISA.
- **Footnote 8 (pg. 7):** can we be provided a copy of the “NZSIS Policy – use and obligations under direct access agreements”?
- **35 (pg. 8):** The IGIS would appreciate being supplied a copy of the quarterly and annual audit by the NZSIS Compliance and Risk team and also a copy of the DIA audit. We suggest that any inappropriate access that involves a breach of privacy is also reported to the Privacy Commissioner.
- **Footnote 11 (pg. 8):** can we have a copy of this SOP?
- **39 and 40 (pg.8):** We feel this should also refer to the Public Records Act 2005 and any relevant internal policies.

- **Risk table 1 (pg. 10):** “the audit log data controlled by NZSIS is available to support security and compliance auditing, both by NZSIS security officers and the IGIS.” Who are the security officers and would the use of this term limit audit access?
- **Risk table 2 (pg. 12):** Under compliance and monitoring, fourth bullet point “unauthorised and/or inappropriate access to DIA Information will be treated as a security breach” should also be reflected in paragraph [35]. Is unauthorised or inappropriate access also treated as a compliance incident?
- **Appendix 2: Privacy Principles (pg. 18):** Under 3, ‘collection of information from subject’ it states “the DAA between the Minister of Internal Affairs and the Minister Responsible for NZSIS is publicly available and makes it clear that NZSIS has access to DIA Information collected by Customs.” For our understanding, can the NZSIS and/or DIA explain what information DIA collects from Customs and why?

31 January 2022

OPC comments on the draft NZSIS/DIA Direct Access Agreement and related PIA

Direct Access Agreement

1. BDMRR Act transition

This refers to definitions in the BDMRR 1995. As that Act is due to be replaced, should the DAA also refer to the BDMRR 2021 so that the Agreement does not become out of date when the new Act comes into force?

2. Definition of citizenship information

Citizenship information is defined in the ISA and the DAA in line with the Citizenship Act as:

citizenship information means information that relates to the acquisition or loss of citizenship by, or to the citizenship status of, any person.

In s 26A(6) of the Citizenship Act, provision for sharing citizenship information with specific government agencies for verification and entitlement purposes expressly includes information as to any change of identity or gender.

That elaboration has not been included for purposes of direct access in the ISA. We recommend clarifying the status of information about change of identity or gender under the DAA, with appropriate safeguards if necessary.

3. Threshold for extraction of DIA information

Clause 8.1 should be amended to reflect that the threshold for collection is that transfer of DIA information is **necessary** for NZSIS purposes as per IPP 1 (rather than **relevant**) and for consistency with aligns with:

- clause 9.1 of DAA – access is **required** to carry out a function, power or duty;
- para 21 of the PIA - NZSIS will only use DIA Information when it is **necessary** for the purposes of undertaking its specific statutory function(s); and
- PIA analysis of IPP 1.

The same amendment is recommended for clause 11.1.2.3 in relation to the transfer of DIA information, and should also be reflected in the PIA risk table.

4. Threshold for further audit

Clause 10.4 provides for a further audit if an annual audit identifies issues of **privacy concern**. As matter of privacy concern is not defined, we recommend more specificity i.e. that the threshold for a further audit should be triggered if an audit indicates access to DIA Information that is not in accordance with the terms of the DAA and operational procedures. We note that a further joint audit is at DIA's discretion which also controls whether a further audit is triggered.

5. Requests for /disclosures of DIA information under other legislation including the Privacy Act

Clause 14.1 now highlights the information privacy principles as an additional means of requesting or disclosing DIA information, however it appears unnecessary to highlight the IPPs as alternative permission for the sharing of DIA statutory register information to which access is regulated by specific legislation; where access to DIA information is comprehensively provided for by the ISA (including the ability to request information under s 121 and the related MPS which mirror the IPPs); and given the statutory safeguards under those statutes.

On that basis we recommend deleting the reference:

Nothing in this agreement affects NZSIS's ability to request information or DIA's ability to disclose information under other provisions in the ISA or where the request or disclosure is authorised or required under any enactment, including the Registration Act or Citizenship Act ~~or as permitted by the information privacy principles~~, however access to DIA Information via this DAA is to be preferred unless it is necessary to request the information via other means.

6. Right of complaint

As clause 18.2 affirms complaint rights to the IGIS, we recommend adding a similar affirmation in clause 18.1 in relation to the right to make a complaint to the Privacy Commissioner:

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

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

Privacy Impact Assessment

1. Registration Information

Footnote 5 of the PIA appears to be inconsistent with the DAA (cl 3.1.7.2) in referring to donor information as related information as included in the Registration Information:

Related information (e.g. registering as a donor in relation to human reproduction, applications to be a civil union or marriage celebrant and instruments of paternity) obtained under other legislation such as the Marriage Act 1955, the Civil Union Act 2004, Status of Children Act 1969, and Human Reproductive Technology Act 2004.

DAA: Registration information does not include:

3.1.7.2 does not include adoption information, witness protection name change information, sexual assignment or correction information to which ss 77(2), (3) or (4) of the Registration Act applies, or **Human Assisted Reproductive Technology Act 2004 donor or donor offspring information.**

2. Reporting misuse

Para 35 should reflect that inappropriate access may also require reporting to the Privacy Commissioner if it amounts to a serious privacy breach under the Privacy Act, as per the risk table, note 13. See also the same comment from the OIGIS.

3. Risk 3 – unauthorised sharing

Note that this may result in a privacy breach as well as a security breach, requiring notification to the Privacy Commissioner if serious, as per risk 2.

4. Analysis of the privacy principles

IPP 6 analysis – note that the right to seek confirmation about personal information is under the Privacy Act, not the OIA which relates to the right to request official information.

IPP 7 analysis – note that the right to correct personal information is under the Privacy Act, not the OIA.

IPP 10 analysis – this analysis should note that the limit in s 220 of the ISA.

IPP 11 analysis

- The ISA analysis should include the limit in s 220 ISA
- The analysis covers both the ISA and the IPP 11 exceptions but is unclear on their relationship i.e. the IPP 11 exceptions are relevant where disclosure is not otherwise authorised by the ISA (recognised by the Privacy Act in section 24(1)). The analysis could be adjusted to reflect

Further, disclosure of personal information by NZSIS may come within the following exceptions exemptions to IPP11:

IPP 12 analysis – third column not completed.

~~IN CONFIDENCE~~



Te Tari Taiwhenua
Internal Affairs



New Zealand
Security Intelligence
Service
Te Pā Whakamarumarū

3 June 2022

Brendan Horsley
Inspector-General of Intelligence and
Security

By email: Brendan.horsley@igis.govt.nz

Liz Macpherson
Acting Privacy Commissioner

By email: enquiries@privacy.org.nz

Tēnā korua Inspector-General and Acting Privacy Commissioner

Registration and Citizenship Information Direct Access Agreement

1. Thank you for your letters dated 28 January 2022 and 1 February 2022 providing comments on our proposed draft direct access agreement.
2. We would particularly like to note the helpful and constructive nature of your combined comments. We were able to address most matters by changes to clarify our position, with the balance then reflected via amendment. We do not consider there are any major points of disagreement remaining.
3. The IGIS response did highlight one particular area that we wish to provide further information on below – but we do not see the implications of that impacting on progression of this agreement, as it reflects an awareness of a particular area of development within the NZIC, and the wider Crown, that is beginning to gain momentum.

Guidance provided on Crown Relationship with Maori under the Treaty of Waitangi

4. The IGIS has raised a query around what guidance is provided to staff around the Crown relationship with Māori under the Treaty of Waitangi. We thought it might be helpful to outline the recent developments in this area for NZSIS (although these equally apply to the GCSB as well).
5. In 2021 Te Tira Tiaki – Government Communications Security Bureau & NZ Security Intelligence Service started their journey of building capability to engage effectively with Māori through the development of a Maihi Karauna – Māori Language Plan. The plan and course of action was accepted by Te Arawhiti (The Office for Māori Crown relations) from whom the organisations received certification.

~~IN CONFIDENCE~~

~~IN CONFIDENCE~~

6. Some of the actions within this plan involve offering NZIC staff guidance and insight into Te Ao Māori via consistent Te Reo Māori courses. It is important to note that the Directors-General also have their own Māori Language Plans and attend classes outside of work hours to lead the community by example.
7. NZIC also provide opportunities to attend Treaty of Waitangi workshops with s6(a) where staff are able to gain a better understanding of the Treaty and how it affects the work of the NZIC.
8. In addition to this, in early 2021 NZIC undertook a series of workshops to assess current level of maturity against Te Arawhiti's Māori Crown Relations Framework.
9. This key work enabled NZIC to see its current state and informed a series of actions to help mature the organisations to better work with, and for, Māori.
10. One of the main actions for the NZIC was to source Māori cultural expertise to guide the community in this space. This has led to the appointment of a Chief Advisor Māori within the NZIC, who started February 2022. This role is currently assessing all areas of NZIC work to inform and shape a meaningful framework underpinned by the Treaty, Public Service Act 2020, UN Declaration on the Rights of Indigenous People and Te Ture mō Te Reo Māori 2016 (Māori Language Act 2016) that will see the NZIC develop and mature in the following key areas:
 - a. As organisations:
 - i. Governance
 - ii. Relationships with Māori
 - iii. Structural considerations
 - iv. Workforce capability
 - v. Environment; and
 - vi. Policy development and service delivery
 - b. As individuals:
 - i. Understanding racial equity and institutional racism
 - ii. NZ history and The Treaty of Waitangi
 - iii. Worldview knowledge
 - iv. Tikanga/kawa
 - v. Te Reo Māori; and
 - vi. Engagement with Māori
11. NZSIS looks forward to maturing as a community from unfamiliar to comfortable, capable and confident.

Incidental matters

12. We attach our particular responses to the other matters identified in your letters in the attached table at Appendix One.

~~IN CONFIDENCE~~

~~IN CONFIDENCE~~

Next steps

13. As noted above we do not consider there to be any remaining points that require further comment or discussion. That being said, if you do have any further comments on the agencies' responses above or in the attached table we invite your comment by 30 June 2022.
14. Alternatively we would be happy to arrange a further meeting with both IGIS and PC staff to discuss further, should you consider there are any outstanding issues.
15. Many thanks for your agencies' constructive comments during this process, we have very much appreciated being able to progress the proposed amendments in a timely fashion even allowing for the difficulties we all have had over the Covid pandemic.

Ngā mihi

s6(a)

General Counsel
NZSIS

s9(2)(a)

Logan Fenwick
Manager Information Partnerships
DIA

~~IN CONFIDENCE~~

~~IN CONFIDENCE~~

Appendix One- Comments Table

Draft Direct Access Agreement

Clause	Comment	Agency	Joint Response
3.1.6	This refers to definitions in the BDMRR 1995. As that Act is due to be replaced, should the DAA also refer to the BDMRR 2021 so that the Agreement does not become out of date when the new Act comes into force?	PC	Agreed. Have updated to refer to the Public Service Act 2020 and both current BDMRR 1995 and 2021.
3.1.7.1	See 3.1.6	PC	Agreed. Have inserted Registration Act definition to generally cover both Act.
3.1.7.2	See 3.1.6	PC	Agreed. Have incorporated 2021 act provisions.
4.1.1	See 3.1.6	PC	Agreed. Definition change above fixes this.
14.1	See 3.1.6	PC	Agreed. Definition change above fixes this.
3.1.2	<p>Citizenship information is defined in the ISA and the DAA in line with the Citizenship Act as:</p> <p>"citizenship information means information that relates to the acquisition or loss of citizenship by, or to the citizenship status of, any person."</p> <p>In s 26A(6) of the Citizenship Act, provision for sharing citizenship information with specific government agencies for verification and entitlement purposes expressly includes information as to any change of identity or gender.</p> <p>That elaboration has not been included for purposes of direct access in the ISA. We recommend clarifying the status of information about change of identity or gender under the DAA, with appropriate safeguards if necessary.</p>	PC	Agreed. Have specifically excluded information as to any change gender as per s26A(6)(b) of the Citizenship Act but any name change information, or citizenship information change following a name change, or any similar identity change is within the scope of this DAA and the safeguards outlined in the DAA would apply to that information.
8.1	<p>Clause 8.1 should be amended to reflect that the threshold for collection is that transfer of DIA information is necessary for NZSIS purposes as per IPP 1 (rather than relevant) and for consistency with aligns with:</p> <ul style="list-style-type: none"> • clause 9.1 of DAA – access is required to carry out a function, power or duty; • para 21 of the PIA - NZSIS will only use DIA Information when it is 	PC	Agreed.

~~IN CONFIDENCE~~

~~IN CONFIDENCE~~

	<p>necessary for the purposes of undertaking its specific statutory function(s); and</p> <ul style="list-style-type: none"> PIA analysis of IPP 1. 		
11.1.2.3	<p>The same amendment [as 8.1] is recommended for clause 11.1 2.3 in relation to the transfer of DIA information, and should also be reflected in the PIA risk table.</p>	PC	Agreed.
10.4	<p>Clause 10.4 provides for a further audit if an annual audit identifies issues of privacy concern. As matter of privacy concern is not defined, we recommend more specificity i.e. that the threshold for a further audit should be triggered if an audit indicates access to DIA Information that is not in accordance with the terms of the DAA and operational procedures. We note that a further joint audit is at DIA's discretion which also controls whether a further audit is triggered.</p>	PC	Agreed.
14.1	<p>Clause 14.1 now highlights the information privacy principles as an additional means of requesting or disclosing DIA information, however it appears unnecessary to highlight the IPPs as alternative permission for the sharing of DIA statutory register information to which access is regulated by specific legislation; where access to DIA information is comprehensively provided for by the ISA (including the ability to request information under s 121 and the related MPS which mirror the IPPs); and given the statutory safeguards under those statutes.</p> <p>On that basis we recommend deleting the reference:</p> <p>"Nothing in this agreement affects NZSIS's ability to request information or DIA's ability to disclose information under other provisions in the ISA or where the request or disclosure is authorised or required under any enactment, including the Registration Act or Citizenship Act or as permitted by</p>	PC	Agreed.

~~IN CONFIDENCE~~

~~IN CONFIDENCE~~

	the information privacy principles, however access to DIA Information via this DAA is to be preferred unless it is necessary to request the information via other means."		
18.1	As clause 18.2 affirms complaint rights to the IGIS, we recommend adding a similar affirmation in clause 18.1 in relation to the right to make a complaint to the Privacy Commissioner: 18.1 Nothing in this DAA affects an individual's right to make an information privacy request in accordance with the Privacy Act 2020 <u>or to make a complaint to the Privacy Commissioner under the Privacy Act.</u>	PC	Agreed.
9.2.1	Can we please confirm if this is a one-time only training or an annual training?	IGIS	Intended to be a one-time only training unless there are significant changes to DIAs systems that would require further training.
9.3	Can we please be provided with a copy of the Joint SOP?	IGIS	Agreed. Will provide once SOP is complete.
9.4	For oversight purposes, the IGIS should have access to this record.	IGIS	Agreed. We will provide quarterly internal audit reports, and then IGIS can request specific access as required. Will also mark the record as within an ACG group the IGIS staff have access to.
10.2	For oversight purposes, the IGIS should have access to this record.	IGIS	As per 9.4
10.3	See 10.2	IGIS	As per 9.4
10.4	For oversight purposes, we recommend that, if there is any significant delay in the yearly audit of this DAA, the IGIS is notified of the delay.	IGIS	Agreed. Generally these are scheduled by the host agency (so DIA in this case) so not usually within our control.
13.5	What guidance is there for NZSIS staff when considering the Crown relationship with Maori under the Treaty of Waitangi?	IGIS	As noted in the main letter this is an area for development within the wider Crown that goes much wider than this agreement. The full impact of <i>Te Pou Matakana Limited v Attorney-General (No 1)</i> [2021] NZHC 2942 (WOCA 1) is yet to be known – and we are expecting both the wider Crown and our own guidance to develop over the next three years, but obviously having much wider application than just the interpretation of this agreement.
13.6	We recommend that this section should reference the relevant Ministerial Policy Statements (i.e. cooperation with overseas public authorities).	IGIS	Agreed.

~~IN CONFIDENCE~~

~~IN CONFIDENCE~~

Draft Privacy Impact Assessment			
Clause	Comment	Agency	Joint Response
13(iii)	We note that this is not a statutory function of the NZSIS, and the statutory functions refer to s 10 and 11 ISA.	IGIS	Agreed. Have clarified by reference to "functions, duties or powers".
16	Will there be a SOP regarding discovery activities conducted by the Service under this DAA?	IGIS	There will be direct access policy relevant to considerations under all DAAs to be contained within our Collections policy, and where required specific guidance notes for a specific DAA. The current draft of the Collection Concepts policy also refers to discovery activities. Both policies once finalised will be provided to the IGIS.
25	We believe that this is a typo and the word should be "international".	IGIS	Agreed.
Footnote 5	<p>Footnote 5 of the PIA appears to be inconsistent with the DAA (cl 3.1.7.2) in referring to donor information as related information as included in the Registration Information:</p> <p>Related information (e.g. registering as a donor in relation to human reproduction, applications to be a civil union or marriage celebrant and instruments of paternity) obtained under other legislation such as the Marriage Act 1955, the Civil Union Act 2004, Status of Children Act 1969, and Human Reproductive Technology Act 2004.</p> <p>DAA: Registration information does not include: 3.1.7.2 does not include adoption information, witness protection name change information, sexual assignment or correction information to which ss 77(2), (3) or (4) of the Registration Act applies, or Human Assisted Reproductive Technology Act 2004 donor or donor offspring information.</p>	PC	Noted. Have simplified and just used the DAA defined terms to avoid confusion.
Footnote 7	According to the ISA, the NZSIS does not have "information assurance and cybersecurity services" functions, and these are the function of the GCSB (s 12). And for ease of use, we also suggest the references in the footnote	IGIS	NZSIS does not have functions under s12 of the ISA, but "information assurance and cybersecurity services" is also within s11 "protective security services, advice, and assistance." Will remove specific reference to information assurance and cybersecurity services. References added.

~~IN CONFIDENCE~~

~~IN CONFIDENCE~~

	are linked to the relevant sections in the ISA.		
Footnote 8	can we be provided a copy of the "NZSIS Policy – use and obligations under direct access agreements"?	IGIS	The policy addressing NZSIS's various collection mechanisms is still under development. This policy incorporates the treatment of Direct Access agreements. We will provide this policy when agreed.
35	The IGIS would appreciate being supplied a copy of the quarterly and annual audit by the NZSIS Compliance and Risk team and also a copy of the DIA audit. We suggest that any inappropriate access that involves a breach of privacy is also reported to the Privacy Commissioner.	IGIS	Agreed. As per 9.4 DAA comment above we will provide. Also agreed to clarify that any notifiable privacy breach will be notified to the PC.
35	Para 35 should reflect that inappropriate access may also require reporting to the Privacy Commissioner if it amounts to a serious privacy breach under the Privacy Act, as per the risk table, note 13. See also the same comment from the OIGIS.	PC	As per above – agreed.
Footnote 11	Can we have a copy of this SOP?	IGIS	Agreed. Will be completed after DAA and PIA are finalised but we will provide a copy once finalised.
39	We feel this should also refer to the Public Records Act 2005 and any relevant internal policies.	IGIS	Agreed.
40	See 39.	IGIS	Agreed.
Risk Table 1	"the audit log data controlled by NZSIS is available to support security and compliance auditing, both by NZSIS security officers and the IGIS." Who are the security officers and would the use of this term limit audit access?	IGIS	This refers to the protective monitoring team within NZSIS. This would not limit the audit function- it's not intended that DIA would know the specific identities of the NZSIS officers using the DAA, but they would know the log-in details attached to the NZSIS officer's that would allow NZSIS to identify staff (or IGIS for that matter) accessing DAA information inappropriately if required. We have further reworded to confirm that the Compliance team (and not only protective monitoring team may also audit).
Risk Table 2	Under compliance and monitoring, fourth bullet point "unauthorised and/or inappropriate access to DIA Information will be treated as a security breach" should also be reflected in paragraph [35]. Is unauthorised or inappropriate access also treated as a compliance incident?	IGIS	Yes. IGIS will note a previous incident was referred to them under a different DAA. Have made explicit in latest draft.

~~IN CONFIDENCE~~

~~IN CONFIDENCE~~

Risk Table 3	Note that this may result in a privacy breach as well as a security breach, requiring notification to the Privacy Commissioner if serious, as per risk 2.	PC	Have brought the relevant notification table from the "compliance and monitoring" section from Risk Table 2 in here to clarify.
Appendix 2	Privacy Principles (pg. 18): Under 3, 'collection of information from subject' it states "the DAA between the Minister of Internal Affairs and the Minister Responsible for NZSIS is publicly available and makes it clear that NZSIS has access to DIA Information collected by Customs." For our understanding, can the NZSIS and/or DIA explain what information DIA collects from Customs and why?	IGIS	This is in error from precedent. Changed "Customs" to "DIA".
IPP 6 analysis	– note that the right to seek confirmation about personal information is under the Privacy Act, not the OIA which relates to the right to request official information.	PC	Agreed. Cannot imagine a situation where s26 OIA might apply here so will remove.
IPP 7 analysis	note that the right to correct personal information is under the Privacy Act, not the OIA.	PC	Agreed as per IPP 6 response above.
IPP 10 analysis	– this analysis should note that the limit in s 220 of the ISA.	PC	Agreed. Paragraph added.
IPP 11 analysis	<ul style="list-style-type: none"> The ISA analysis should include the limit in s 220 ISA The analysis covers both the ISA and the IPP 11 exceptions but is unclear on their relationship i.e. the IPP 11 exceptions are relevant where disclosure is not otherwise authorised by the ISA (recognised by the Privacy Act in section 24(1)). The analysis could be adjusted to reflect 	PC	Re: s220 – agreed and paragraph added. Re: IPP 11 analysis – agreed and changes made, and similar changes incorporated into IPP 12.

~~IN CONFIDENCE~~

~~IN CONFIDENCE~~

	Further, disclosure of personal information by NZSIS <u>may</u> come within the following <u>exceptions</u> exemptions to IPP11:		
IPP 12 analysis	- third column not completed.	PC	Noted and completed.

~~IN CONFIDENCE~~