



New Zealand
Security Intelligence
Service
Te Pā Whakamarumaru

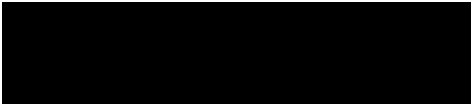
New Zealand
Security Intelligence Service
PO Box 900, Wellington

P +64 4 472 6170

F +64 4 472 8209

www.nzsis.govt.nz

27 January 2023



Tēnā koe [REDACTED]

Official information request

Thank you for your Official Information Act 1982 (OIA) request of 16 November 2022, transferred from the office of Hon Andrew Little to the New Zealand Security Intelligence Service (NZSIS) on 29 November 2022. The part of your request transferred to the NZSIS was for:

- The September 15, 2022 document "*Briefing Note – Direct Access to DIA Information by NZSIS*"

I note you were advised on 17 January 2023 that the time limit for responding to your request had been extended to 31 January 2023 because the consultations necessary to make a decision on your request were such that a proper response could not reasonably be made within the original time limit.

Response

Please find a copy of the briefing *Direct access to DIA Information by NZSIS* enclosed. A small amount of information has been withheld under the following sections of the OIA:

- Section 6(a), where the making available of the information would be likely to prejudice the security or defence of New Zealand or the international relations of the Government of New Zealand; and
- Section 9(2)(a), as the withholding of the information is necessary to protect the privacy of natural persons, including that of deceased natural persons.

Where section 9 grounds have been applied I do not consider that the need to withhold this information is outweighed by other considerations which render it desirable, in the public interest, to make that information available.

In addition, you will note that the briefing note refers to draft versions of the Direct Access Agreements and Privacy Impact Assessment Reports being enclosed. Both restricted and unclassified versions of these documents were provided to the Ministers with these briefings. The restricted versions need to be withheld under section 6(a) of the OIA, as outlined above. However, unclassified versions of these documents have been published on the NZSIS's website at <https://www.nzsis.govt.nz/about-us/working-with-others/>. Accordingly, insofar as your request relates for the unclassified versions of this information, I am refusing

these parts of your request under section 18(d) of the OIA, as the information is publicly available.

Review

If you wish to discuss this decision with us, please feel free to contact uia.privacy@nzsis.govt.nz.

You have the right to seek an investigation and review by the Ombudsman of this decision. Information about how to make a complaint is available at www.ombudsman.parliament.nz or freephone 0800 802 602.

Please note that the NZSIS proactively publishes OIA responses in accordance with the expectations of Te Kawa Mataaho/the Public Service Commission. We intend to publish this letter (with your personal information removed) and enclosed documents on the NZSIS's website. Publication of such responses is done on a quarterly basis.

Ngā mihi



Rebecca Kitteridge

Te Tumu Whakarae mō Te Pā Whakamarumaru
Director-General of Security

~~RESTRICTED~~

DMS20-7-21571



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.

~~RESTRICTED~~

~~RESTRICTED~~

DMS20-7-21571

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).

~~RESTRICTED~~

~~RESTRICTED~~

DMS20-7-21571

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~~

~~RESTRICTED~~

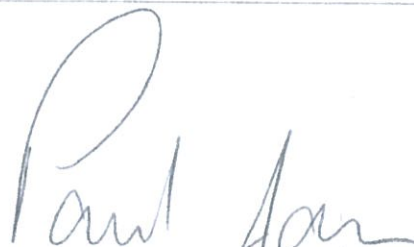
Recommendations

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 Whakamarumaru

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 Māori 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) 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	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.	PC	Agreed.
10.4	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.	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 re-worded 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~~

	<u>Further</u> 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~~