New Zealand Security Intelligence Service
Te Pā Whakamarumaru

New Zealand Department of Internal Affairs

DIA Information

Privacy Impact Assessment Report

Owner	Knowledge Manager
Approved By	Chief Privacy Officer
Approval Date	18 October 2022
Review Date	18 October 2022

Contents

Part 1: Relevant Legislation....3
Part 2: NZSIS Responsibilities....3
Using DIA Information....3
Protecting DIA Information....3
NZSIS ownership....4
Part 3: Scope....4
Part 4: Use of DIA Information....4
NZSIS will only use DIA Information to fulfil its statutory functions....5
NZSIS will use DIA Information in a way that is necessary and proportionate....6
Part 5: Protecting DIA Information....6
Secure data ingestion and storage....6
Access to DIA Information....6
Disclosure of DIA Information to other parties....8
Retention /deletion of DIA Information....8
Part 6: Privacy risks and mitigations....8
RISK 1....10
RISK 2....11
RISK 3....14
RISK 4....15
Part 7: Compliance and Audit Requirements....16
Appendix 1: NZSIS Roles and Responsibilities....17
Appendix 2: Privacy Principles....18

Part 1: Relevant Legislation

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

2. An update to the Direct Access Agreement (DAA) between the Minister Responsible for NZSIS and the Minister of Internal Affairs came into effect on 18 October 2022 after being signed by both parties on 18 October 2022.

3. The DAA enables NZSIS to access Registration Information stored on the BDM Database (held by the Registrar-General) and Citizenship Information stored on the Citizenship Database (held by the Secretary for Internal Affairs). Both databases are stored by the Department of Internal Affairs (DIA), will be accessed by NZSIS in the same way, and subject to the same safe-guards, and will collectively be referred to as **DIA Information**.[1]

Part 2: NZSIS Responsibilities

4. NZSIS direct access to DIA Information must comply with the terms of the DAA, as signed by the Minister of Internal Affairs and the Minister responsible for NZSIS.[2]

Using DIA Information

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

    i. any DIA Information is used[3] only for the purposes of NZSIS statutory functions as set out in the ISA; and

    ii. any DIA Information obtained under the DAA is used in a way that is necessary and proportionate to NZSIS functions.

Protecting DIA Information

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

    i. clear procedures for accessing, using, disclosing and retaining DIA Information;

---

[1] Any reference to DIA Information includes:
   a. the data held in the BDM and Citizenship databases (including information related to request for particular information held on those databases); and
   b. all of its computer components, including software, underlying data repositories, and any system interface required to access the database information.

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

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

ii. clear measures for protecting the privacy of individuals identified by DIA Information; and

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

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

NZSIS ownership

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

Part 3: Scope

In scope

9. This Privacy Impact Assessment (PIA) report should be read in conjunction with the updated DAA between the Minister Responsible for NZSIS and the Minister of Internal Affairs. This PIA report:

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

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

Out of scope

10. This PIA does not cover any potential access to DIA Information by the Government Communications Security Bureau (GCSB) or any other agency.

Part 4: Use of DIA Information

11. DIA Information is collected for the purposes of maintaining a series of statutory registers. The nature and scope of information contained in these registers is wide ranging and includes a record of citizens by birth but for the purposes of the DAA the following are the relevant types of information with definitions as covered in the DAA:

    i. Registration Information; and

    ii. Citizenship Information.

12. The NZSIS utilises DIA Information for the purposes of maintaining and enhancing New Zealand's national security.

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

NZSIS will only use DIA Information to fulfil its statutory functions

13. NZSIS uses DIA Information to fulfil the following statutory functions, duties or powers, of the organisation:

    i. Intelligence collection and analysis;

    ii. Protective security services, advice and assistance;

    iii. Acquiring, use or maintenance of an assumed identity; and requests for assistance to acquire, use and maintain an assumed identity.

Intelligence collection and analysis

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

15. NZSIS staff utilise DIA Information to help verify identities to enable the ability to further investigations into people of national security interest.

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

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

Providing protective security services, advice and assistance to partner agencies

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

    i. advice about national security risks (for example, in support of citizenship, immigration and border security decision-making processes, usually by request of another agency); [5]

    ii. supporting decision-making around the suitability of individuals to be granted a national security clearance (for example through the vetting process); and

    iii. preventing, detecting and responding to risks to national security presented by individuals with access to sensitive or classified information (this may include maintenance of the national security clearance database).

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

Acquiring, use or maintenance of an assumed identity; and requests for assistance to acquire, use and maintain an assumed identity

19. NZSIS may access DIA Information in order to conduct checks to ensure NZSIS does not create or amend an assumed identity (or request another agency (that may include DIA) to create or amend an assumed identity) which is an exact match with someone of the same name and birth date born in New Zealand.

20. For avoidance of doubt no requests for DIA to create or amend an assumed identity will be made under this DAA.

NZSIS will use DIA Information in a way that is necessary and proportionate

21. NZSIS will only use DIA Information when it is necessary for the purposes of undertaking its specific statutory function(s).[6]

22. The way in which the NZSIS uses DIA Information must be proportionate to the activity it is undertaking. The benefit of using the DIA Information for the purposes of undertaking NZSIS's statutory functions must outweigh the potential intrusion of privacy that may result from NZSIS acquiring and retaining information extracted from the databases.

Part 5: Protecting DIA Information

Secure data ingestion and storage

23. NZSIS access DIA Information from DIA via stand-alone DIA supplied terminals located within NZSIS facilities. The terminals operate as standard remote terminals according to DIA standard remote access capabilities. The terminals operate over a fully encrypted virtual private network (VPN). The VPN provides an additional layer of security and encryption for DIA Information.

24. DIA Information assessed as relevant to NZSIS's statutory functions is transferred by the Authorised Officer to NZSIS's security accredited Top Secret network for processing, storage and future use.

25. Access to the NZSIS network is strictly controlled in accordance with international security standards for intelligence and security agencies. It is only accessible by staff who have been security vetted to the highest level (Top Secret Special).

Access to DIA Information

26. NZSIS staff may access DIA Information in two ways:

    i. Direct access to DIA Information via a DIA terminal; and

[6] NZSIS functions include intelligence collection and analysis (s10 of the ISA), protective security services, advice and assistance (s11 of the ISA), , cooperation with other public authorities to facilitate their functions (s13 of the ISA) and cooperation with other entities to respond to imminent threat (s14 ISA).

ii. access to DIA Information which has been ingested into NZSIS intelligence systems.

27. Only Authorised Officers have access to DIA terminals. Both access methods have unique access restriction mechanisms, to ensure DIA Information is accessed by those authorised to do so for the purposes of undertaking NZSIS's statutory functions.

28. Direct access to DIA Information via a DIA terminal is limited to Authorised Officers only.

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

30. NZSIS has clear operational procedures for Authorised Officers regarding when and how they may access DIA Information.[7]

31. Access to DIA Information is controlled by a defined query, Authorised Officers will not have access to browse DIA Information.

Access to DIA Information held within NZSIS intelligence systems

32. Access to DIA Information held within NZSIS systems is limited to NZSIS employees working directly in intelligence and security roles[8] as well as a small number of staff in enabling functions (compliance, information management, legal advisors, IT administration, etc.). This access is not authorised until the employee has successfully completed mandatory Direct Access compliance training, obtained sign off from their Line Manager and confirmation from the NZSIS Compliance and Risk team.

Access auditing

33. User access to DIA Information is captured in two ways:

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

    ii. automated audit log data for DIA Information obtained under the DAA accessed via NZSIS intelligence systems.

34. **DIA Register of Use:** each instance of access[9] to DIA Information via a DIA terminal must be recorded in the DIA Register of Use by the Authorised Officer. Failure to record activity in the DIA Register of Use may result in a breach of the conditions of use of DIA system, which may result in the termination of the Authorised Officer's DIA account and/or access privileges.

35. The DIA Register of Use is held on the NZSIS system and is audited by the NZSIS Compliance and Risk team on a quarterly basis to ensure that Authorised Officers are

[7] NZSIS Policy- Use and obligations under direct access agreements
[8] This includes security clearance vetting.
[9] 'Access' refers to any activity requiring the user to log in to the DIA terminal; this includes each search undertaken by the Authorised Officer **and** also captures the action of the log in itself.

compliant with DIA record keeping requirements. NZSIS also provide the DIA Register of Use to DIA on an annual basis for additional auditing against DIA system records.

36. Any misuse of the DIA system, including inappropriate access to DIA Information by an NZSIS employee, will be reported to DIA and the Inspector General of Intelligence Services (IGIS) in line with NZSIS processes for compliance incidents and will also be treated as a security breach. Any notifiable privacy breach will also be notified to the Privacy Commissioner.

37. **Automated audit logs:** All access to DIA Information by NZSIS staff is monitored by the DIA. Audit data is used to support security and compliance auditing.[10]

Disclosure of DIA Information to other parties

38. Authorised Officers must not access DIA Information on behalf of other agencies (with the exception for being when conducting assumed identity function noted at paras 19-20 above on behalf of GCSB), except as part of a statutory NZSIS function (and this may include the provision of protective security service, advice and assistance such as when conducting pre-employment checks on behalf of the New Zealand Intelligence Community (NZIC)).

39. DIA Information may be provided to other New Zealand government departments or overseas intelligence partners by virtue of it being incorporated into an intelligence report.[11] Any such information sharing will be conducted in accordance with the DAA, as well as Ministerial Policy Statements and NZSIS policies. In addition when considering whether to share information, NZSIS will give due consideration to the Crown's relationships with Māori under the Treaty of Waitangi.

Retention /deletion of DIA Information

40. NZSIS will fulfil its statutory obligations and act in accordance with the Public Records Act 2005, any Ministerial Policy Statement regarding the retention or destruction of information and as those obligations are set out in internal policy.[12]

Retaining DIA Information

41. Information which has been retrieved from DIA under the DAA and is required to support the statutory functions of NZSIS is ingested into NZSIS's systems (for example its intelligence analysis system) and managed as a business record of NZSIS activities and subject to any Public Records Act 2005 requirements.

Disposing of Information

42. All NZSIS business records are subject to an agreed disposal authority issued by the Chief Archivist.

Part 6: Privacy risks and mitigations

[10] Auditing BDMI and Citizenship access by NZSIS Authorised Officers – SOP
[11] For example to verify an individual's identity or in support of joint investigative work.
[12] NZSIS Policy - Data Retention & Disposal under the ISA

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

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

Impacts	*Summary of mitigations*		
DIA Information captures a large volume of personal information about New Zealand citizens and foreign nationals. Unauthorised access to this information by an external party (a member of the public or a hostile foreign intelligence service hacking into the information) may result in the following impacts • a major breach of the Privacy Act 2020 • significant negative impact on public trust and confidence in NZSIS and the reputation of NZSIS • significant negative impact on the relationship between NZSIS and DIA • possible that DIA Information could be used by a hostile actor to enhance their own capabilities and/or undermine the national security of New Zealand	NZSIS takes extensive steps to ensure DIA Information is transferred and stored securely. **Data transfer** • transfer of DIA Information from DIA to NZSIS is conducted via an encrypted virtual private network (VPN). • the VPN provides an additional layer of security and encryption for DIA Information. **Data storage + systems access** • all DIA Information retention and access is conducted on NZSIS's Top Secret network access to DIA systems is controlled with user login by Authorised Officers only. • access to the NZSIS network is strictly controlled in accordance with New Zealand and Five Eyes security standards for Top Secret networks • access is only granted to people working for NZSIS, all of whom have been security vetted to the highest level (Top Secret Special) **Systems Certification and Accreditation (C&A)** • the NZSIS network is classified at Top Secret(the highest level of government network security) and is fully security accredited by GCSB **Access auditing** • all access by NZSIS staff (including system administrator access) to DIA Information generates detailed audit log data, and this will be the same for investigative analysis searches conducted on DIA Information • the audit log data controlled by NZSIS is available to support security and compliance auditing, both by NZSIS security or compliance officers and the IGIS		
	Residual Risk Rating		
	Likelihood: RARE	Impact: CRITICAL	Residual Risk Rating: **MEDIUM**

RISK 2
Unauthorised and/or inappropriate access to DIA Information by an NZSIS employee

Impacts	*Summary of mitigations*
DIA Information captures a large volume of personal information about New Zealand citizens and foreign nationals. Unauthorised and/or inappropriate access to DIA Information by an NZSIS employee may have a range of impacts, depending on the nature and the extent of access. This could include, but is not limited to A breach of the Privacy Act 2020 resulting in interference with the privacy of one or more individuals • moderate impact on public trust and confidence in NZSIS and the reputation of NZSIS • minor impact on the relationship between NZSIS and DIA 'Access' or 'use' of DIA Information includes any activity requiring the user to log in to the DIA system, even if the only action is the log in itself.	NZSIS takes extensive steps to ensure DIA Information is only accessed by authorised NZSIS employees for appropriate purposes. ***Systems mitigations*** **Access to the DIA terminal (Authorised Officer)** • access to DIA Information is strictly limited to Authorised Officers only (See Appendix 1 for definition) **Access to DIA Information held in NZSIS systems is limited by Access Control Group (ACG) settings** • NZSIS intelligence analysis systems limit access to DIA Information to NZSIS staff who have received training in the identification of data obtained by direct access and who have signed a briefing acknowledging their responsibilities in respect of this information. **Access auditing** • the **Authorised Officer** must record each search they undertake of DIA Information through the DIA terminal in the DIA Register of Use. • the DIA Register of Use is maintained by the **NZSIS Compliance and Risk team** and is audited on a regular basis to ensure that **Authorised Officers** are compliant with the record keeping requirements outlined in *ID – Using the DIA System SOP* • NZSIS will provide the DIA Register of Use to DIA on an annual basis for additional auditing against DIA system records, to ensure NZSIS access to DIA Information is in keeping with the DAA • any misuse of the DIA terminal, including inappropriate access to DIA Information by a NZSIS employee, will be reported to the Inspector General of Intelligence and Security (IGIS) and DIA in line with NZSIS processes for compliance incidents • failure to record use could result in a breach of the conditions of use of the DIA terminal and termination of the user's and/or NZSIS's access privileges. ***Operational mitigations*** **Training** • all NZSIS staff must complete information management training, including training on their responsibilities in searching for and accessing information appropriately. This training also makes NZSIS employees aware of their information management obligations under the Intelligence and Security Act 2017, the Public Records Act 2005, the Privacy Act 2020, the Official Information Act 1982 and the Ministerial Policy Statement (MPS) on information management

	• Specific training on identifying Direct Access information is mandatory for all NZSIS staff who need to access intelligence information as part of their role
	• Authorised Officers receive additional role-specific training, which includes detailed instruction relating to accessing and using DIA Information
	
	Managerial oversight
	• NZSIS managers are responsible for ensuring employees are aware of their obligations and only access information that is reasonably required to enable them to carry out their official duties as part of NZSIS's functions
	
	Compliance and monitoring
	• NZSIS Privacy Officers are responsible for advising the **NZSIS Chief Privacy Officer** and the SLT on the adequacy of NZSIS systems for dealing with personal information and compliance with the Privacy Act and steps to be taken to promote robust privacy practices.
	• a dedicated NZSIS Compliance Team oversees the development, implementation and compliance with relevant policies, including information management and access policies
	  • NZSIS has a dedicated security team with full access to all audit log data, whose responsibilities include investigating anomalous access to any NZSIS information
	  • unauthorised and/or inappropriate access to DIA Information will be treated as a security breach and a compliance incident.
	• Where an internal investigation confirms a privacy breach, and it is considered necessary or required by law,[13] the relevant affected parties (including NZSIS and DIA) and/or the Office of the Privacy Commissioner will be notified as soon as possible. NZSIS will also inform the Inspector General of Intelligence and Security.
	
	Strategic mitigations
	
	Policies, Standard Operating Procedures (SOPs) and user agreements
	  • all NZSIS employees with access to DIA Information must comply with the access and usage requirements outlined in NZSIS Policy and SOP documentation, which reflect the requirements of the DIA Direct Access Agreement
	• all NZSIS employees must read and sign an Information Technology and Information Systems Agreement for General Users
	  • all NZSIS employees must read and sign the NZSIS Code of Conduct, which outlines requirements for access to sensitive information contained within NZSIS systems
	• failure to comply with NZSIS policies, SOPs, user agreements and/or the NZSIS code of conduct will be investigated and may result in disciplinary action.
	
	Internal work programmes

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

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

RISK 3
Unauthorised and/or inappropriate sharing of DIA Information with a domestic or international agency

Impacts	*Summary of mitigations*
Sharing DIA Information with external agencies (both domestic and international) is routine practice for NZSIS. NZSIS share DIA Information with external agencies in order to meet a range of operational requirements, including • to verify an individual's identity • to obtain further details, or • to progress joint national security investigations. Unauthorised and/or inappropriate sharing of DIA Information with an external agency may have a range of impacts depending on what information is shared and who it is shared with. This could include, but is not limited to: A breach of the Privacy Act 2020 resulting in serious harm to one or more individuals	NZSIS takes extensive steps to ensure all information shared with external agencies, including DIA Information obtained via direct access, is shared in a way that is authorised and appropriate. **Training** • NZSIS staff must complete mandatory training regarding Information Management and Human Rights • NZSIS employees must complete the Information Management training module as soon as possible following induction. NZSIS employees who regularly interact with overseas parties with must complete Human Rights risk management training following induction and must refresh their training on an annual basis; these training modules outline the human rights risk management policy which applies to the activities of NZSIS, and details how this policy is applied when data is shared with international agencies. **Procedural mitigations** • DIA Information may only be provided by NZSIS to other New Zealand government departments or overseas intelligence partners in accordance with the Intelligence and Security Act 2017 (ISA), NZSIS policies and SOPs and the DAA requirements. • NZSIS Managers are responsible for ensuring that any information released to external agencies (both foreign and domestic) meets NZSIS information sharing requirements. Any unauthorised and/or inappropriate sharing of information derived from DIA under the direct access agreement with an external agency would be treated as a security breach and prompt an investigation, in which DIA would be consulted. Security breach investigations may lead to disciplinary action. **Compliance and monitoring** • NZSIS Privacy Officers are responsible for advising the **NZSIS Chief Privacy Officer** and the SLT on the adequacy of NZSIS systems for dealing with personal information and compliance with the Privacy Act and steps to be taken to promote robust privacy practices. • a dedicated NZSIS Compliance Team oversees the development, implementation and compliance with relevant policies, including information management and access policies • NZSIS has a dedicated security team with full access to all audit log data, whose responsibilities include investigating anomalous access to any NZSIS information • unauthorised and/or inappropriate access to DIA Information will be treated as a security breach and a compliance incident.

• significant negative impact on public trust and confidence in NZSIS and the reputation of NZSIS • significant negative impact on the relationship between NZSIS and DIA	• Where an internal investigation confirms a privacy breach, and it is considered necessary or required by law,[14] the relevant affected parties (including NZSIS and DIA) and/or the Office of the Privacy Commissioner will be notified as soon as possible. NZSIS will also inform the Inspector General of Intelligence and Security. **Systems mitigations** • NZSIS can only share information with external agencies via secure information sharing mechanisms • all information sharing mechanisms generate detailed audit log data, which is available to support security and compliance auditing • physical transfer of information off the network for the purposes of sharing the information with an external agency must be authorised and comply with NZSIS information security standards		
	Residual Risk Rating		
	Likelihood: RARE	Impact: MODERATE	Residual Risk Rating: **LOW**

RISK 4
DIA Information is retained for longer than necessary within NZSIS systems

Impacts	***Summary of mitigations***		
Retention of DIA Information (and therefore personal information) for longer than necessary would be contrary to IPP9 and may constitute a moderate breach of the Privacy Act 2020.	All DIA Information that is brought into the NZSIS intelligence analysis system is information that has featured in a legitimate NZSIS function and is maintained as a business record in accordance with a disposal authority issued by the Chief Archivist.		
	Residual Risk Rating		
	Likelihood: LIKELY	Impact: MINOR	Residual Risk Rating: **MEDIUM**

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

Part 7: Compliance and Audit Requirements

44. DIA and NZSIS will undertake a joint audit of the operation of this DAA at least once per year, in accordance with a jointly agreed audit procedure. A copy of this audit report will be provided to the Inspector-General of Intelligence and Security and also to the Office of the Privacy Commissioner if there are any significant privacy concerns.

45. DIA can also review access by **Authorised Officers** to the DIA terminal at any time.

46. The information provided to DIA will not include details of NZSIS operations and investigations but will include the statutory functions being exercised and the purposes for which DIA Information was accessed.

ENDS

Appendix 1: NZSIS Roles and Responsibilities

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

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

    i. the management and flow of information, including DIA Information management;

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

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

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

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

    iii. promoting robust privacy practices across NZSIS; and

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

4. The **Manager Strategy and Accountability** is responsible for:

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

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

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

    i. acting as the operational lead for access to and use of DIA Information by NZSIS teams; and

    ii. liaising with the DIA Service Delivery and Operations Risk and Assurance staff to conduct the annual joint audit of NZSIS access to DIA Information under the DAA.

6. An **Authorised Officer** is as defined in the DAA.

Appendix 2: Privacy Principles

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

    i. fulfil our obligations under the DAA;

    ii. fulfil our obligations under the Privacy Act 2020;

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

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

Table 1. NZSIS Privacy Principles Assessment

	Privacy Principle as per the Privacy Act	NZSIS assessment against privacy principle	Compliance with Privacy Principle?
1	**Purpose of the collection of personal information** *Collection of personal information by an agency must be lawful and necessary to the function of the agency*	NZSIS has access to DIA Information for the purpose of undertaking its statutory functions. NZSIS access to DIA Information is **lawfully** authorised under the Schedule 2 of the Intelligence and Security Act (ISA) 2017. Information is considered **necessary** where it is required to support the performance of NZSIS' statutory functions • intelligence collection and analysis • protective security services, advice, and assistance • co-operation with other public authorities to facilitate their functions • co-operation with other entities to respond to imminent threat	Compliant
2	**Source of personal information** *Get it directly from the people concerned wherever possible.*	If NZSIS were to collect DIA Information from the individual, this may • be prejudicial to the maintenance of the law; • prejudice the purposes of the collection; and • would not be reasonable practicable in the circumstances NZSIS is exempt from PP2 under s28 of the Privacy Act; however, NZSIS access to DIA Information via the DIA is lawful as per Schedule 2 of the ISA.	Exempt under s28 of the Privacy Act
3	**Collection of information from subject** *Tell them what information you are collecting, what you're going to do with it, whether it's voluntary, and the consequences if they don't provide it.*	The DAA between 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 DIA. While it is public knowledge that NZSIS have **access** to DIA Information, details of exactly how NZSIS **uses** DIA Information are not available to the public in order to protect national security practices. For this reason, NZSIS is exempt from PP3 under s28 of the Privacy Act 2020.	Exempt under s28 of the Privacy Act

4	**Manner of collection of personal information** Personal information shall not be collected by an agency (a) by unlawful means; or (b) by means that, in the circumstances of the case (i) are unfair; or (ii) intrude to an unreasonable extent upon the personal affairs of the individual concerned. *Be fair and not overly intrusive in how you collect the information*	PP4(a): NZSIS access to DIA Information is lawful as per Schedule 2 of the ISA PP4(b): NZSIS access to DIA Information is exempt from PP4(b) under s28 of the Privacy Act	Compliant with PP4(a) Exempt from PP4(b) under s28 of the Privacy Act
5	**Storage and security of personal information** *Take care of it once you've got it and protect it against loss, unauthorised access, use, modification or disclosure and other misuse*	All DIA Information is ingested and stored on a fully security accredited Top Secret network. NZSIS take extensive measures to ensure storage and access to DIA Information is secure.	Compliant

6	**Access to personal information** *People can see their personal information if they want to*	Under the Privacy Act 2020, an individual has the right to seek confirmation from both DIA and NZSIS about whether personal information is held about them. The Registrar-General and the Secretary for Internal Affairs are responsible for the collection of DIA Information from the source. As the "holder agency", the Registrar-General or the Secretary for Internal Affairs are best place to handle information requests from individuals regarding their DIA Information. Any personal and/or official information requests to NZSIS regarding DIA Information not held by NZSIS will be transferred to DIA. Any DIA Information that is brought into the main NZSIS intelligence analysis system following an investigative analysis query will be considered by NZSIS through their standard information request process. Any requests to DIA regarding access to DIA information by NZSIS should be transferred to, or consulted with, NZSIS as appropriate to mitigate any potential risk to national security.	Compliant
7	**Correction of personal information** *They can correct it if it's wrong, or have a statement of correction attached.*	Under the Privacy Act 2020, an individual has the right to request that their personal information is amended if it is incorrect. The DIA are best place to handle requests from individuals regarding corrections to their DIA Information. Any requests to NZSIS regarding corrections to an individual's DIA Information will be transferred to DIA. DIA will notify NZSIS should this result in the correction of any DIA Information obtained by NZSIS under the DAA.	Compliant
8	**Accuracy etc. of personal information to be checked before use** *Make sure personal information is correct, relevant and up to date before you use it*	DIA have established procedures to ensure the accuracy of DIA Information most notably that most information registered is provided by the source of the information. Usually this will be from the subjects of the information or in the case of birth registration by the parents. NZSIS operational procedures require employees to undertake rigorous analysis of the individual's case against intelligence holdings to confirm their identity **before** acting on DIA Information.	Compliant
9	**Not to keep personal information for longer than necessary** *Get rid of it once you're done with it.*	Any DIA Information that is brought into the main NZSIS intelligence analysis system following an investigative analysis query is maintained as a business record of NZSIS, with disposal arrangements as agreed in disposal authority DA692.	Compliant

10	**Limits on use of personal information** *Use it for the purpose you collected it for, unless one of the exceptions applies.*	PP10 states that an intelligence and security agency that holds personal information that was obtained in connection with one purpose may use the information for any other purpose (a secondary purpose) if the agency believes on reasonable grounds that the use of the information for the secondary purpose is necessary to enable the agency to perform any of its functions. The use of DIA Information for protective security functions and intelligence collection and analysis is necessary to enable NZSIS to perform its statutory functions. This use is therefore permitted under exemptions under IPP10, including (c)(i) to avoid prejudice to the maintenance of the law; (d) public health or public safety; (e) directly related to the purpose in connection with which the information was obtained. Should NZSIS obtain any information under the DAA for the purposes of a security clearance assessment then the limitation on further use of that information under section 220 of the ISA will apply.	Compliant

11	**Limits on disclosure of personal information** *Only disclose it if you've got a good reason, unless one of the exceptions applies*	Under s10 of the ISA, NZSIS is authorised to provide any intelligence collected and any analysis of that intelligence to the Minister, the Chief Executive of DPMC, and any person or class of persons (whether in New Zealand or overseas) authorised by the Minister to receive the intelligence and any analysis. Under section 11 of the ISA, NZSIS is authorised to, amongst other things, provide advice and assistance to any public authority (whether in New Zealand or overseas), any person or class of persons (whether in New Zealand or overseas) authorised by the Minister. This protective security services, advice, and assistance includes for the purposes of providing advice and assistance around personnel, information, and physical security, as well as advice around national security risks. Under s13 of the ISA, NZSIS is authorised to cooperate with other New Zealand government departments Under section 14 of the ISA, NZSIS is authorised to provide advice and assistance to anyone responding to an imminent threat to the life or safety of any person in New Zealand, or any New Zealand citizen or permanent resident overseas, any person in any area that New Zealand has search and rescue responsibilities for, or any person outside the territorial jurisdiction of any country. Should NZSIS obtain any information under the DAA for the purposes of a security clearance assessment then the limitations on further use of that information under section 220 of the ISA will apply. Any information sharing undertaken by NZSIS is conducted in accordance with the DAA, as well as Ministerial Policy Statements and NZSIS policies. In circumstances where disclosure of the information is not otherwise authorised by the ISA, as recognised by the Privacy Act at s 24(1), disclosure of personal information by NZSIS comes within the following exceptions to IPP11: (a) disclosure is one of the purposes (or directly related) for which information was obtained; (e) non-compliance is necessary to avoid prejudice to the maintenance of the law or for Court proceedings; (f) necessary to prevent or lessen a serious threat. (g) that the disclosure of the information is necessary to enable an intelligence and security agency to perform any of its functions.	Compliant

12	**Disclosure of personal information outside New Zealand**	Under s10 of the ISA, NZSIS is authorised to provide any intelligence collected and any analysis of that intelligence to the Minister, the Chief Executive of DPMC, and any person or class of persons (whether in New Zealand or overseas) authorised by the Minister to receive the intelligence and any analysis. Under section 11 of the ISA, NZSIS is authorised to, amongst other things, provide advice and assistance to any public authority (whether in New Zealand or overseas), any person or class of persons (whether in New Zealand or overseas) authorised by the Minister. This protective security services, advice, and assistance includes for the purposes of providing advice and assistance around personnel, information, and physical security, as well as advice around national security risks. Under section 14 of the ISA, NZSIS is authorised to provide advice and assistance to anyone responding to an imminent threat to the life or safety of any person in New Zealand, or any New Zealand citizen or permanent resident overseas, any person in any area that New Zealand has search and rescue responsibilities for, or any person outside the territorial jurisdiction of any country. Any information sharing undertaken by NZSIS is conducted in accordance with the DAA, as well as Ministerial Policy Statements and NZSIS policies. In circumstances where disclosure of the information is not otherwise authorised by the ISA, as recognised by the Privacy Act at s 24(1), disclosure of personal information by NZSIS outside New Zealand is for the purposes of IPP11(g). However, should sharing disclosure outside of New Zealand occur in reliance on IPP 11(a), (c), (e), (f), (h), or (i) then IPP 12 would apply. (g) that the disclosure of the information is necessary to enable an intelligence and security agency to perform any of its functions.	Compliant
13	**Unique identifiers** *Take care when using unique identifiers*	DIA Information obtained under the DAA and transferred into NZSIS's main intelligence analysis system will be identifiable as personal information; no unique identifiers will be generated except those required by the intelligence analysis system to function as a database	Compliant