The following is summarised information from the New Zealand Security Intelligence Service Data Retention and Destruction under the ISA policy. Where possible, excerpts of the original document have been used. Some details are withheld under section 6(a) of the Official Information Act 1982 as release would prejudice national security.

NZSIS Data Retention and Destruction under the ISA

Introduction

- The functions of the New Zealand Security Intelligence Service (NZSIS) include:
    - Intelligence collection and analysis;
    - Providing protective security service, advice, and assistance (including security vetting);
    - Co-operating with other public authorities to facilitate their functions; and
    - Co-operating with other entities to respond to imminent threats.
- Effective management of the information NZSIS holds to carry out these functions is vital for core business and compliance with legislative obligations.
- The NZSIS has a number of obligations related to information management contained within legislation and the Ministerial Policy Statement ('MPS') on *the management of information obtained by GCSB and NZSIS, including retention and disposal of that information.* This policy focuses on the **data retention and destruction** obligations contained under the Intelligence and Security Act 2017 ("the ISA").

Scope

- This policy only covers data retention and destruction obligations that apply to information obtained:
    - Under an **authorisation**;
    - Through a **business record direction**;
    - Through an application to access **restricted information**; and
    - Through a **direct access agreement**.
- This policy must be read and understood by all NZSIS employees. In particular, it must be applied by employees who are responsible for requesting, approving or collecting information using the methods listed above.

Policy

- This section outlines retention and disposal obligations in accordance with the ISA.

Unauthorised information

- Unauthorised information is:
    - Information unintentionally obtained that is outside the scope of –
        - An authorisation; or
        - An authorised activity; or
    - Information obtained by NZSIS during the provision of co-operation, advice and assistance under section 14, where the mechanism for obtaining the information would normally require a warrant.

Irrelevant information

- NZSIS has a positive obligation under section 103 of the ISA to destroy certain types of "irrelevant" information as soon as practicable.
- Irrelevant information is information that:
    - Is obtained by NZSIS within the scope of an authorised activity; but
    - Is not required, or no longer required, by NZSIS for the performance of its functions.
- There is also an obligation under section 152 to destroy business records obtained under a business record direction as soon as practicable if the records are not required, or are no longer required, by NZSIS to perform its functions.
- Information collected under an authorisation, received through a business record direction or permission to access restricted information must be assessed for relevance as soon as practicable. Where the information is assessed to be relevant to the performance of NZSIS statutory functions, then it may be retained.
- Where there is uncertainty regarding the relevance of the information, or the material needs to be retained for further assessment, it may be kept for the maximum period listed within the NZSIS Data Retention Plan ('DRP').

Incidentally obtained information

- Incidentally obtained information is information that is collected by the NZSIS (either under a warrant or without the need for a warrant) when performing:
    - Intelligence collection and analysis; or
    - Protective security services
- However, the information obtained is not relevant to those functions of the NZSIS and therefore should be destroyed.
- The only circumstance where it would be appropriate to retain incidentally obtained information, which will be for the purpose of disclosure, is where it may be relevant to:
    - Prevent or detect serious crime in New Zealand or any other country;
    - Prevent or respond to threats to the life of any person in New Zealand or any other country;
    - Identify, prevent or respond to threats or potential threats to the security or defence of New Zealand or any other country; or
    - Prevent the death of any person who is outside territorial jurisdiction of any country.
- The information may be retained for the purpose of disclosure to the New Zealand Police, New Zealand Defence Force or any other public authority.

Revoked authorities

- The responsible Minister, and Commissioner of Intelligence Warrants may at any time amend or revoke an intelligence warrant or business record approval and direct that all or any specific information obtained under the warrant or business record approval before it was amended or revoked be destroyed. The NZSIS must comply with this direction as soon as practicable. During the period of time it takes to destroy the information, it must not be used.

Direct Access

- Under the ISA, the NZSIS can obtain direct access to specified public sector databases where they have a 'direct access agreement' with the database holder. The

agreement will specify the terms governing NZSIS direct access – including the use, access, retention and disclosure of any information obtained from the database.

Directing information to be destroyed

- The NZSIS will provide a system and guidance to support employees to destroy information in accordance with the provisions in this policy.

Annex 1 – NZSIS Data Retention Plan

The NZSIS Data Retention Plan specifies the timeframes for determining the relevance of information. These timeframes do not apply to unauthorised information, which must be destroyed immediately after it has been identified.

Annex 2 – Relevant Legislation

The ISA includes specific provisions under Part 4 Subpart 4 regarding unauthorised and irrelevant information.