Ministerial Policy Statement

Information management

Summary

It is necessary for employees of GCSB and NZSIS to collect information, including personal information, in the course of performing their statutory functions.

This MPS provides guidance for employees on the management of that information, including its retention and disposal.

In making decisions related to information management, employees must have regard to the following principles: necessity and proportionality, security of information, privacy protection, shared responsibility, and oversight. This MPS also specifies certain additional matters to be included in internal policy and procedures.

Definitions

The Act *means the Intelligence and Security Act 2017,*

Disposal *is defined in the Public Records Act 2005 and means the transfer of control of a record or the sale, alteration, destruction, or discharge of a record.*

Information *means data and information obtained, collected, created and/or managed by GCSB and NZSIS in the performance of statutory functions under the Intelligence and Security Act 2017, through any method, including warranted and lawful unwarranted collection methods.*

Information management / Management of information *means the processes of recording, storing, reviewing, disposing of, and sharing information for the purpose of performing one or more statutory functions of GCSB and NZSIS.*

Personal information *means information about an identifiable individual as defined by section 7 of the Privacy Act 2020.*

Privacy principles *are the information privacy principles contained in Part 2 of the Privacy Act 2020.*

Privileged communications or privileged information *means communications or information protected by legal professional privilege or privileged in proceedings under section 54 or any of sections 56 to 59 of the Evidence Act 2006.*

Public record / Record *are defined in the Public Records Act 2005.*

Context

1. To perform their statutory functions, GCSB and NZSIS (the agencies) obtain and use a wide variety of information, including at times personal information. The effective management of this information throughout the collection, analysis, storage, protection, dissemination, and disposal phases is vital for GCSB and NZSIS's core business, as well as meeting legal obligations. Sound information management policies and practices are also important to minimise the intrusiveness of the agencies' information collection.

Sources of Information

2. Parts 4 and 5 of the Act allow GCSB and NZSIS to lawfully collect information using a variety of methods, some of which may be covert and without the knowledge of any person(s) about which information has been collected.
3. Information may be collected under an intelligence warrant or other authorisation or through other lawful collection methods (that do not require specific authority) such as using human sources, publicly available information, surveillance in a public place, and the provision of information assurance and cybersecurity services. The conduct of collecting information using these means is addressed in a number of related MPSs (refer to MPSs on *Collecting human intelligence, Publicly available information, Conducting surveillance in a public place and Information assurance and cybersecurity activities)*.
4. GCSB and NZSIS may also obtain information from foreign partners (refer to MPS on *Cooperating with overseas public authorities*).

Legal Framework

5. All government agencies are subject to legislative requirements under the Public Records Act 2005, the Privacy Act 2020 and the Official Information Act 1982 (the OIA) to retain, protect and, where appropriate, provide access to information. GCSB and NZSIS are subject to additional obligations under the Act regarding the handling of information that is unauthorised, irrelevant or incidentally obtained.

Public Records Act 2005

6. In accordance with section 17 of the Public Records Act, GCSB and NZSIS are required to create and maintain full and accurate records of their affairs and retain all information they receive or create in the conduct of their affairs until authorised for disposal. All public records and information should be available in an accessible form until disposal is authorised.[1]
7. All public records deemed to be of long-term archival value must be transferred into the control of the Chief Archivist 25 years after the date of their creation, unless a deferral of transfer has been obtained. Deferrals of transfer for GCSB and NZSIS records can be obtained either through the agreement with the Chief Archivist or, through the certification of the Minister in consultation with the Minister responsible for Archives New Zealand, for any records which could be prejudicial to the maintenance of New Zealand's security, defence or laws, or an individual's safety.

---

[1] *Public records can only be disposed of with the authority of the Chief Archivist or if required by another Act, such as the Intelligence and Security Act 2017 (section 18, Public Records Act 2005). Disposal may occur by transferring control, altering or destroying, selling or discharging the public record (section 20, Public Records Act 2005).*

Privacy Act 2020

8. The Privacy Act promotes and protects individual privacy, by setting out the principles for how public sector agencies should collect, use, disclose and allow access to personal information (the privacy principles).
9. Due to the nature of some of the agencies' collection methods (including the need to collect information about an individual without their awareness), GCSB and NZSIS are exempt from principles 2, 3, and 4(b) of the Privacy Act.[2]
10. Due to their statutory functions, GCSB and NZSIS have specific exceptions that apply to principles 10 and 11. These exceptions relate to using information that has been collected for one purpose for limited secondary purposes, and disclosing information if it is reasonably necessary to perform a statutory function.
11. Section 47 of the Privacy Act ('decision to neither confirm nor deny personal information is held') provides a response to requests for access to personal information under Principle 6.

Official Information Act 1982

12. GCSB and NZSIS have an obligation under the OIA to make official information available when requested, unless there is a good reason for withholding it under sections 6 (conclusive reasons), 7 (special reasons), or 9 (other reasons). A national security classification is not in itself a justification for withholding information requested under the OIA. Sections 10 (neither confirming nor denying the existence or non-existence of information) and 18 (refusal of requests) provide additional responses to requests for information.

Intelligence and Security Act 2017

13. The Act contains a number of provisions relating specifically to information obtained and held by GCSB and NZSIS, which operate in conjunction with obligations under the Public Records Act and Privacy Act. These include:
    - The obligation to destroy as soon as practicable all information obtained under an urgent or very urgent authorisation if that authorisation is subsequently revoked (including by operation of law), unless section 104 applies (sections 76 and 81);
    - The obligation to immediately destroy unauthorised information (information unintentionally obtained that is outside the scope of an authorisation or authorised activity), unless a warrant is obtained as soon as practicable or section 104 applies (section 102);
    - The obligation to destroy as soon as practicable information that is obtained within the scope of an authorised activity but is irrelevant to the performance of the agency's functions, unless retention is required by any other laws or court orders (section 103);
    - The ability to retain incidentally obtained information that is not relevant to a function (whether obtained through an authorisation or other means), only for the purposes of disclosing that information to the New Zealand Police, New Zealand Defence Force, or other public authority in order to assist them to fulfil their own statutory functions related to serious crime, threat to life, threats to the security or defence of New Zealand

[2] *Section 28 of the Privacy Act 2020.*

or another country, or the death of any person outside the territorial jurisdiction of any country (section 104);

    - The obligation to destroy as soon as practicable all business records information obtained under a business records direction if the records are irrelevant to the performance of the agency's functions, unless retention is required by any other laws or court orders (section 152); and
    - The obligation to act in a manner that ensure democratic oversight (section 17(d)) and to make all security records accessible to the Inspector General of Intelligence and Security (section 217).

- The Act also establishes a number of offences (which carry fines of up to $10,000, or imprisonment of up to two years and a fine of up to $10,000) relating to the unlawful use and disclosure of information held by GCSB and NZSIS. It is important that GCSB and NZSIS have information management practices and procedures in place that protect information from being used in any manner that would constitute one or more of these offences, regardless of whether that is by current or former employees, or any other person.

Guidance for GCSB and NZSIS

Scope

14. This MPS applies to all information obtained, collected, created and/or managed by GCSB and NZSIS in the course of exercising their statutory functions. It focusses, in particular, on information that is held by GCSB and NZSIS as a result of their intelligence collection and analysis, and protective security and cybersecurity functions. It includes information intercepted, seized, copied or otherwise obtained under a warrant or authorisation (issued under Part 4 of the Act) or other lawful means that do not require a warrant (including but not limited to those methods specified in Parts 3 and 5 of the Act). Information may include video recordings and photographic images (and their metadata), as well as data obtained from electronic tracking.
15. This MPS does not specifically address records that fall under General Disposal Authority 6 (Common corporate service public records) and General Disposal Authority 7 (Facilitative, transitory, and/or short-term value records) issued by the Chief Archivist under the Public Records Act 2005.

Principles

16. The Directors-General of GCSB and NZSIS are responsible for the management and use of information obtained by the agencies in the course of performing their statutory functions. They must have in place policies and procedures that ensure such information is used for those purposes and in compliance with the law.
17. The following principles constitute a framework for good practice and are to be taken into account by GCSB and NZSIS when developing internal information management policies and procedures:

Necessity and Proportionality

18. All activities relating to information obtained by GCSB and NZSIS under their intelligence, protective security and cybersecurity functions must be necessary and proportionate. Proportionate activity should use the least intrusive means to meet the purpose of the activity, taking into account the extent and sensitivity of personally identifiable information obtained and the potential impact on third parties.
19. From time to time the GCSB and NZSIS will inevitably obtain information that is within the scope of an authorised activity but not required for the performance of statutory functions. This is explicitly recognised by the destruction provisions contained within Subpart 4 of Part 4 of the Act. GCSB and NZSIS must have guidelines in place to assist employees to determine whether information is required for the performance of statutory functions – either immediately or in the longer term (for example, as part of ascertaining a pattern of communications between persons of interests over time).
20. If agencies obtain information by unintentionally exceeding the scope of an intelligence warrant, that information is covered by section 102 of the Act and must be destroyed immediately. An exception to this obligation is that GCSB and NZSIS may retain information that is not relevant to their statutory functions only for the purpose of disclosing it to another agency for the performance of that agency's statutory functions in accordance with the requirements of section 104 of the Act. This includes where there are reasonable grounds to believe that the information may assist in: preventing or detecting serious crime; preventing or responding to threats to life; and identifying, preventing or responding to threats or potential threats to the security or defence of any country.
21. Information that has been disclosed to the Police, New Zealand Defence Force or other public authority under section 104 should be retained by the disclosing agency as a public record of the disclosure unless destruction obligations under sections 102 and 103 apply. If retained, such information will no longer be available for intelligence purposes, strict access controls will apply and the information will be subject to the Public Records Act 2007.

Security of Information and Management of Access

22. All information obtained, collected, created and/or managed by GCSB and NZSIS must be stored in an appropriate repository/repositories, reflecting the sensitivity of the information and level of protections required. Electronic storage systems must be accredited in accordance with relevant standards outlined in the New Zealand Information Security Manual (NZISM). It must also ensure future access to the information, and, in the case of information gained from overseas public authorities, operate in accordance with the originators' requirements.
23. In addition to technical information security measures, GCSB and NZSIS must ensure that all access to information is for authorised purposes only. Information must have a classification in accordance with the New Zealand Government Security Classification System, and consequential storage and handling requirements must be adhered to.
24. Access to information obtained by GCSB and NZSIS should be limited to the minimum number of people that are required to see it for the purposes of performing the statutory functions of the agencies. In other words, there must be a positive reason for access to information.

25. Access control systems and procedures must include having the ability to log who has accessed information and when, and to identify unauthorised access to information. Unauthorised access includes when an employee is authorised to access information but has done so for purposes other than to fulfil a statutory function which is within that employee's remit or has done so for the purposes of providing the information to an unauthorised party.

Shared Responsibility

26. Good information management practice is the shared responsibility of all employees, regardless of the role an employee has in GCSB and NZSIS. Every employee must be aware of, and follow, information management policies and procedures in the course of their work. GCSB and NZSIS have a general duty to create and capture full and accurate records,[3] as well as to maintain and manage those records, in compliance with those policies and procedures.

Compliance and Oversight

27. Effective information management practices facilitate and support compliance with the record keeping and retention and disposal obligations under the Public Records, Privacy and Intelligence and Security Acts. They are also essential to facilitate effective oversight of GCSB and NZSIS by the Inspector-General of Intelligence and Security, to respond effectively to government inquiries, and to support decisions to release/decline requests for access to information under the Privacy Act and OIA. GCSB and NZSIS information management policies and procedures must be able to support effective responses to requests by the Inspector-General of Intelligence and Security, the Office of the Privacy Commissioner, the Office of the Ombudsman and the Chief Archivist.

Matters to be reflected in internal policies and procedures

28. GCSB and NZSIS must have, and act in compliance with, internal policies and procedures that are consistent with the requirements and principles of this MPS and have systems in place to support and monitor compliance.
29. Those policies and procedures must also address the following additional matters set out below.

Review, Retention, Disposal, and Transfer Schedules

30. GCSB and NZSIS must have policies and processes that provide guidance on the retention and destruction of information that give effect to the requirements of the Intelligence and Security Act Public Records Act and Privacy Act. Policies should assist the agencies to:
    - identify and destroy unauthorised and/or irrelevant information in accordance with the requirements of the Act and Principle 9 of the Privacy Act 2020;
    - retain information that has been distinguished as required for as long as it remains required for a business purpose related to a statutory function, or is required to be retained as a public archive (under Disposal Authority 692, for example, which relates to GCSB, NZSIS and National Security Group of the Department of Prime Minister and

[3] *Section 17(1) of the Public Records Act 2005.*

Cabinet records), and destroy information that is not required or no longer required; and

- provide indicative timeframes in which the above determinations must be completed.

31. The agencies must specify retention periods for intelligence, protective security and cyber security information that are proportionate to the nature of the information and the purpose for which it was collected or created. Agencies must have procedures in place to ensure that information that has reached the end of any retention timeframe is destroyed or brought forward for review, and be able to justify any continued retention. Continued retention for a further period must be shown to be necessary and proportionate.

Privileged Information

32. GCSB and NZSIS are prohibited from obtaining privileged communications or privileged information of New Zealanders and permanent residents of New Zealand under intelligence warrants. However, there may be times when such information is unintentionally collected. GCSB and NZSIS must have policies in place that address the need to protect statutorily prescribed classes of privileged information, as outlined in section 70 of the Act, to ensure the protections that apply in relation to that information are complied with. These protections include the obligation to destroy (without reporting) any privileged material relating to New Zealanders that is unintentionally obtained or collected. The Directors-General must ensure that all employees who could potentially handle privileged information receive training on the nature of relevant privileges and the applicable policies.
33. In addition to the classes of privileged information in section 70 of the Act, the agencies should be aware of parliamentary privilege with respect to activity affecting Members of Parliament. Agencies should have policy or other documentation to govern agency activity in respect of members of Parliament.

Recording Information

34. GCSB and NZSIS must have procedures for recording information accurately, to the best knowledge of those recording it, and in a manner that will allow it to be used to fulfil statutory functions.

Audit Procedures

35. GCSB and NZSIS must conduct periodic internal audits to ensure compliance with internal policies and procedures and relevant legislation. As a public office, GCSB and NZSIS will also be subject to independent audit of recordkeeping practices as required under the Public Records Act.

Compliance with the Information Privacy Principles

36. GCSB and NZSIS are subject to information privacy principles 1, 4(a), and 5 to 13 of the information privacy principles in the Privacy Act 2020. All policies relating to the management of personal information obtained by GCSB and NZSIS must incorporate guidance about compliance with the information privacy principles in terms of collection, access, accuracy, security, correction, use and disclosure, and retention of personal information by GCSB and

NZSIS. GCSB and NZSIS are required to inform the Privacy Commissioner of notifiable privacy breaches.

37. GCSB and NZSIS will ensure additional protection is given to information that is particularly sensitive, such as that relating to sensitive category individuals4 or security vetting records.

38. The Agencies should also consider any access controls required once public records have been transferred to Archives New Zealand. Under the Public Records Act, GCSB and NZSIS must set the access status of information and the period of any restrictions for records that are transferred to Archives New Zealand or that are 25 years old.

Training

39. Employees of GCSB and NZSIS must be provided mandatory training on relevant law, policies and procedures relating to information management, as applicable. Training should be provided to existing employees and to new employees at induction, and whenever there are significant changes to the policies and procedures, to ensure that employees are at all times aware of current practices. Training in some areas may be targeted, for example, training relating to privileged information should be targeted at employees who could potentially handle privileged information.

Authorisation Procedures

40. The Directors-General of GCSB and NZSIS are to issue the policies and procedures to guide information management by the agencies. Disposal actions must only be taken in accordance with approved Disposal Authorities (general or agency-specific) issued by the Chief Archivist, or as otherwise required by law.

Duration of Ministerial Policy Statement

41. This MPS will take effect from 01 March 2022 for a period of three years. The Minister who issued an MPS may, at any time, amend, revoke or replace the MPS.

Ministerial Policy Statement issued by:

Hon Andrew Little

Minister Responsible for the Government Communications Security Bureau
Minister Responsible for the New Zealand Security Intelligence Service
01 March 2022

---

[4] Sensitive category individuals include, for example, children and young people under 18 years of age, people vulnerable by reason of illness or other incapacity, New Zealand Members of Parliament, members of the New Zealand Judiciary and journalists.