



# Ministerial Policy Statement

## Section 121 requests

### Summary

The Act expressly recognises the existing ability of GCSB and NZSIS to request information from other agencies.

This Ministerial Policy Statement (MPS) provides guidance on making requests under section 121 of the Act. In making these requests GCSB and NZSIS must have regard to the following principles: necessity, proportionality, respect for privacy, less intrusive means to be considered, use of most appropriate statutory mechanism, and oversight. This MPS also specifies certain matters to be included in internal policy and procedures.

#### **Definitions**

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

**Agency** means any person, whether in the public sector or the private sector, and includes a department and an interdepartmental venture.

**GCSB** means the *Government Communications Security Bureau*.

**Information privacy principles** are the information privacy principles contained in the *Privacy Act 2020*.

**NZSIS** means the *New Zealand Security Intelligence Service*.

**Personal information** means information about an identifiable individual.

### Context

#### **Making requests under Section 121 occurs within a wider information collection context**

1. GCSB and NZSIS obtain or collect information through a range of methods authorized under the Act in order to perform their statutory functions. These authorities include:
  - a) Intelligence warrant;
  - b) Business records directions;
  - c) Authorisations to access restricted information; and
  - d) Direct access agreements.

2. GCSB and NZSIS also collect information through means that do not require a specific legal authorisation, including:
  - a) Through the disclosure of information - this may be provided in a number of ways, including:
    - i. unsolicited, without any prior request from GCSB or NZSIS;
    - ii. in response to a request from GCSB or NZSIS under section 121 of the Act (this MPS);
    - iii. by collecting, requesting and receiving information from a person (known as human intelligence activities) (guidance on how GCSB and NZSIS should obtain information directly from persons without an intelligence warrant is addressed the *Collecting human intelligence MPS*);
    - iv. from overseas public authorities (*Cooperating with overseas public authorities MPS*);
  - b) Obtaining, collecting and using publicly available information (*Publicly available information MPS*) and;
  - c) Through the conduct of other lawful activities, such as conducting surveillance in a public place (*Conducting surveillance in a public place MPS*).

### ***Making a request under section 121***

3. In order for GCSB and NZSIS to carry out their functions, they must collect information using a variety of methods, including by requesting information from a range of individuals and organisations for a wide range of reasons. For example, GCSB and NZSIS may request information to facilitate a counter-terrorism investigation or to support the development of operational capability.
4. The Act expressly recognises the existing ability of GCSB and NZSIS to request information held by another agency, including personal information, in order to perform their functions. A Director-General may request information from any other agency where they believe on reasonable grounds that the information is necessary to enable the performance of any of its functions. A request under section 121 must provide details of the information requested and confirm the information is necessary to enable GCSB or NZSIS to perform any of their functions.
5. A request for information under section 121 is not legally enforceable (ie it is a request for voluntary disclosure), and an agency receiving a request may decide whether or not to disclose the information.

### ***Voluntary disclosure of information under section 122***

6. Section 122 recognises the existing ability of an agency to disclose information it holds to the GCSB and NZSIS. Agencies may disclose information (in response to a request or at their own initiative) if they have reasonable grounds to believe that the information is necessary to enable GCSB or NZSIS to perform any of its functions.
7. Information may not be disclosed under section 122 if there is other legislation that prohibits or restricts the disclosure of information to GCSB and NZSIS. If another statutory provision regulates the way in which the information may be obtained or made available to GCSB and NZSIS, then the terms of that provision will prevail. Agencies also remain subject to any

obligations of confidence, or contracts, agreements or other documents relating to the disclosure of the specific information.

8. The Privacy Act 2020 also applies to the voluntary disclosure of personal information. Principle 11 of the Privacy Act states that information should not be disclosed unless one or more of the specified grounds for disclosure applies. This includes where the agency believes on reasonable grounds that disclosure is one of the purposes, or directly related to the purposes in connection with which the information was collected. There is also a specific exception that allows agencies to disclose information to the GCSB and NZSIS where they believe on reasonable grounds the information is necessary to enable them to perform their functions (see information privacy principle 11(1)(g)).
9. To help an agency decide whether to disclose information on the basis it is necessary for GCSB or NZSIS to perform its functions, the relevant Director-General may certify in writing that disclosure of the information is necessary to enable GCSB or NZSIS to perform its functions (section 122(3)).

## Guidance for GCSB and NZSIS

### *Scope of this MPS*

10. The guidance in this MPS does not apply to every request for information made by GCSB and NZSIS. The guidance applies to declared requests<sup>1</sup> for information that GCSB and NZSIS make under section 121 in relation to their investigative and/or operational activity. This may include requests for:
  - a) information about a person, place or other subject of intelligence interest;
  - b) information to support the development of operational capabilities; and
  - c) information about security arrangements or capabilities to inform the provision of protective security services, advice or assistance.
11. For any request to overseas public authorities the MPS on *Cooperating with overseas public authorities* should be considered.
12. The guidance in this MPS does not apply to requests for information if they:
  - a) relate to routine government administrative activities and business functions that are common to most public service departments (such as procurement and employment processes);
  - b) are in a non-declared manner (i.e. it is not disclosed that the requestor works for GCSB or NZSIS);
  - c) are made by the GCSB to facilitate the provision of consented information assurance and cybersecurity activities under section 11 of the Act (covered in the *Information assurance and cybersecurity activities MPS*); or

---

<sup>1</sup> Section 121 requests cannot be covert or undeclared as they must confirm that the requested information is necessary to enable the performance of one or more of GCSB's/NZSIS's functions.

- d) are made by the GCSB to facilitate its regulatory function under Part 3 of the Telecommunications (Interception Capability and Security) Act 2013 (TICSA).<sup>2</sup>
13. GCSB and NZSIS will seek legal advice if there is uncertainty about whether a section 121 request is appropriate in the circumstances.

### ***Principles***

14. The following principles constitute a framework for good decision-making and must be taken into account by GCSB and NZSIS when making requests for information under this MPS. Requests for information (to the extent they are ongoing or repeated) should be subject to regular review as to whether they continue to be consistent with these principles.

### ***Necessity***

15. Requests for information under this MPS should only be made when the information sought is necessary to enable GCSB or NZSIS to perform one or more of its functions. For the avoidance of doubt, this includes requests for information to assess the validity of lines of enquiry or leads. To the extent requests are for personal information, this reflects the law in relation to personal information. [Privacy principle 1](#) of the Privacy Act 2020 provides that personal information should not be collected unless the information is being collected for a lawful purpose connected with a function or activity of the agency and the collection of the information is necessary for that purpose.
16. Requests must be prepared so that they target the information that is necessary and do not seek to capture irrelevant information.

### ***Proportionality***

17. The information requested should be proportionate to the purpose for which the information is sought. For example, a request for a large amount of information, relating to a large number of people, or relating to sensitive personal information, needs to be carefully justified. This will require considering the importance of the purpose for obtaining that information (such as intelligence of importance to the Government of New Zealand, or about immediate or significant threats) and the impacts of collection (such as any privacy or third party impacts) including steps to minimize those impacts.

### ***Respect for privacy***

18. GCSB and NZSIS are subject to the Privacy Act 2020 and [privacy principles](#) 1, 4(a), and 5 to 13 will apply to requests for (and handling of) personal information.
19. GCSB and NZSIS must take reasonable steps to mitigate the impact on the privacy of the person who is the subject of the request. Such steps may include defining the scope of requests for personal information to ensure no more than is necessary is sought, retaining as little personal information as possible when it is supplied, restricting the number of people who may access that information, establishing processes to ensure that information is only accessed for a function of the GCSB or NZSIS and only disclosing that information where there is a legitimate need.

---

<sup>2</sup> Part 3 of the TICSA establishes a framework under which network operators are required to engage with the GCSB about changes and developments with their networks where these intersect with national security.

20. Whether a reasonable expectation of privacy exists requires consideration of all the circumstances, including factors like the nature of the information, the nature of the relationship between the agency to which the request is directed and the person who is the subject of the information, where the information was obtained, and the manner in which the information was obtained. People are more likely to have a reasonable expectation of privacy for information that would reveal intimate details of their lifestyle and personal choices.
21. Where a reasonable expectation of privacy arises, section 21 of the New Zealand Bill of Rights Act 1990 will apply and it will be necessary to consider the reasonableness of the proposed request. Seeking legal advice should be considered in such cases.

#### *Least intrusive means to be considered*

22. GCSB and NZSIS should seek to obtain information by the least intrusive means reasonably available. The intrusiveness of requests for information vary according to the particular information requested and the wider context of the situation. Section 121 requests are voluntary, subject to other legal obligations, and can be tailored to the specific intelligence requirements. As such, they may often be the least intrusive method of obtaining information.
23. However, GCSB and NZSIS should consider whether any alternative collection mechanisms are more appropriate in the specific circumstances to provide additional procedural protections to any affected individual. For example, a section 121 request may be considered less intrusive than warranted methods of collection for the agency receiving the request, but such a request may be more intrusive from the perspective of the person who is the subject of the request due to the lesser procedural protections that are in place, if the requirements for a warrant can be met.
24. GCSB and NZSIS may need to obtain information from multiple sources, using a range of means in order to assess the accuracy of information, or the reliability of sources. For example, in order to reliably assess the state of a person's finances (and the honesty of that person) as part of vetting them for a security clearance, it may be necessary to request information from the person themselves, and other persons who are aware of their financial situation.

#### *Use of most appropriate statutory mechanism*

25. Generally, the Act is designed to operate as a toolkit from which the GCSB and NZSIS may use any appropriate mechanism for obtaining information. For example, section 119 makes it clear that the ability to request information under section 121 does not limit GCSB and NZSIS from collecting personal information if authorised or required by or under another enactment or permitted by the information privacy principles.
26. Where the Act or another enactment provides a specific mechanism (other than an authorisation under Part 4 of the Act) for GCSB or NZSIS to access certain information, there is a general expectation that those mechanisms be used unless there is good reason to make a request under section 121. This is because the procedural safeguards applying to other statutory mechanisms are specifically designed to protect individual privacy interests in those circumstances. For example, if a direct access agreement between NZSIS and/or GCSB and another public sector agency is in place for information about travel movements, GCSB

and NZSIS should normally use that mechanism instead of making a request under section 121.

27. However, the existence of a specific statutory mechanism does not prevent GCSB and NZSIS from making a request under section 121 if there are operationally good reasons to do so such as urgent requests or where it is appropriate to inform the use of those other mechanisms (e.g. seeking confirmation that the individual is a customer of an agency before seeking further information about the individual via a specific statutory mechanism).

### *Oversight*

28. GCSB and NZSIS must carry out all activities in a manner that facilitates effective oversight. Given the wide range of possible section 121 requests, the exact form of a request (e.g. written or verbal) will depend on the operational needs of a situation, the nature of the relationship with the agency and the nature of the information sought.
29. GCSB and NZSIS must keep records of section 121 requests and the response to those requests appropriate to the context and nature of the request. For example, in some circumstances an email chain between GCSB or NZSIS and another agency may constitute an appropriate record of a section 121 request and its response. In other circumstances a record of meeting, file note, or exchange of letters will be the appropriate record of the request and response.
30. Section 123 of the Act requires the Directors-General to keep a register of all certificates issued under section 122(3). It also specifies the information that must be recorded in the register of certificates. The register plays an important role in supporting GCSB, NZSIS, the Inspector-General of Intelligence and Security, and the responsible Minister to monitor and review use of certificates issued under section 122(3).

### ***Matters to be reflected in internal policies and procedures***

31. As public service agencies, GCSB and NZSIS must comply with legislation, policies and procedures common to all New Zealand public service agencies.<sup>3</sup>
32. In addition, 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 must have systems in place to support and monitor compliance.
33. These policies and procedures must also address the following matters:

### *Compliance with the State Services Code of Integrity and Conduct*

34. Consistent with the State Services *Standards of Integrity and Conduct*, the GCSB and NZSIS will not permit individual employees to request information about any person or matter that they have a personal interest in or relationship with (for example, a family member or friend, or where the employee has a personal financial interest in a matter), except when:
  - a) there is a specific reason why it is necessary for that particular employee to request the information for the performance of a statutory function; or
  - b) there are no other persons reasonably available to make the request.

---

<sup>3</sup> This includes the *Public Service Act 20220* and the *Health and Safety at Work Act 2015*.

### *Training*

35. GCSB and NZSIS employees may only make requests for information under section 121 if they are appropriately trained on relevant policies and procedures. Those employees must receive ongoing training to ensure they have up-to-date knowledge of those policies and procedures.

### *Information management*

36. Information received as the result of a request under section 121 may be sensitive or personal information and GCSB and NZSIS must handle and store that information in accordance with clear access controls that correspond to the sensitivity of the information. The *Information Management MPS* applies in relation to management of this information.

### *Compliance with information privacy principles*

37. GCSB and NZSIS are subject to information privacy principles 1, 4(a), and 5 to 13 in the Privacy Act 2020. Policies about requests made under section 121 of the Act must incorporate guidance about compliance with the relevant information privacy principles.

### *Sensitive category individuals*

38. GCSB and NZSIS must have a policy setting out the restrictions and protections necessary in the conduct of activities in respect of sensitive categories of individuals (for example, children and young people aged 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).
39. Authorisation at a high level within GCSB or NZSIS is required for activities conducted in respect of these individuals. This will provide reassurance that appropriate measures are in place in the event that requests for information need to be made to, or in relation to, sensitive category individuals.

### *Information protected by privilege*

40. GCSB and NZSIS must have a policy setting out the restrictions and protections necessary in the conduct activities that may involve communications protected by privilege (for example, communications attracting legal privilege, privilege for communications with ministers of religion and communications attracting medical privilege).

### **Authorisation procedures**

41. Requests for information must be authorised by an appropriately senior employee of the GCSB or NZSIS, having regard to the nature of the information requested, the persons affected by the request (such as sensitive category individuals), the agency it is requested from, the relationship between that agency and GCSB or NZSIS, and any risks associated with making the request.

***Duration of ministerial policy statement***

42. 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:

A handwritten signature in blue ink that reads "Andrew Little". The signature is written in a cursive, flowing style.

**Hon Andrew Little**

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

**01 March 2022**