

## UNCLASSIFIED

torture in all circumstances and will not commit torture nor be complicit in torture committed by others.

15. New Zealand is also a long-standing opponent of the death penalty. New Zealand has abolished the death penalty within its jurisdiction and is committed to promoting global prohibition.<sup>4</sup> The position of the government is that the death penalty is the ultimate form of cruel, inhuman and degrading treatment. New Zealand will not cooperate on specific investigations where the cooperation will lead to a person being sentenced to death, unless there are appropriate assurances that the death penalty will not be carried out.<sup>5</sup>
16. The many positive benefits of New Zealand's participation in foreign intelligence and security relationships do not override New Zealand's legal obligations with respect to human rights.

### **Guidance for GCSB and NZSIS**

17. This section sets out guidance for the agencies when undertaking foreign cooperation. All cooperation must be carried out in accordance with New Zealand law and the principles contained within this MPS. Cooperation with overseas public authorities should be regularly reviewed to ensure cooperation remains consistent with the principles below.

### **Principles**

---

18. These principles constitute a basis for good decision-making and best practice conduct and need to be considered before, during and after cooperation with overseas public authorities.

### **Respect for human rights**

19. GCSB and NZSIS must ensure that their cooperation with overseas public authorities is in accordance with all human rights obligations recognised by New Zealand law. The Directors-General of GCSB and NZSIS must ensure the agencies remain informed of the human rights practices and potential risks related to cooperation with overseas public authorities.
20. There is an expectation that GCSB and NZSIS will undertake critical assessments of human rights risks and have a policy in place to ensure employees know how to assess risk and respond appropriately. To ensure the agencies' cooperation will not result in a real risk of contributing to, or being complicit in, a breach of human rights, this policy must address the risk assessment framework set out below, and provide guidance on when and how the framework is to be applied.

#### *Risk assessment framework*

- 1) *Assess general risk:* Assess the country or public authority's record and practice towards human rights and international humanitarian law. This assessment can include the country or public authority's stability, and where relevant, the success of any previous mitigation efforts that have

---

<sup>4</sup> Under the Second Optional Protocol to the International Covenant on Civil and Political Rights aiming at the abolition of the death penalty.

<sup>5</sup> See s27(2)(ca) Mutual Assistance in Criminal Matters Act and s30(3) of the Extradition Act 1999.

## UNCLASSIFIED

been applied by New Zealand or close international partners when cooperating with the country or authority. See Appendix One for other factors the agencies should take into account.

- 2) *Risk arising from the proposed cooperation:* Consider whether the proposed cooperation, whether one-off or on-going, might result in a real risk of significantly contributing to or being complicit in a breach of human rights. The agencies must take a precautionary approach in making such assessments.
- 3) *Opportunity for mitigating risk:* Where it is identified that there is a real risk of a human rights breach occurring as a result of the proposed cooperation, GCSB and NZSIS should consider whether the risk can be mitigated, for example through conditions or restrictions on the cooperation provided, or through assurances or caveats on the intelligence exchanged.
- 4) *Response to a real risk of human rights breach:* If, following the steps above, there remains a real risk that the cooperation will significantly contribute to, or amount to complicity in, a breach of human rights, cooperation must be refused or referred to the Minister Responsible for the GCSB and NZSIS for a decision. To inform the Minister's decision-making, the information identified in the steps above must be documented and provided to the Minister, along with a clear statement on the purpose of the proposed cooperation. In circumstances where a decision is put to the Minister, the agencies will notify the Inspector-General of Intelligence and Security.

### *Use of intelligence obtained through human rights breaches*

21. GCSB and NZSIS must not request or use intelligence where they know, or assess there is a real risk the intelligence was obtained through a serious human rights breach – such as torture, or cruel, inhuman or degrading treatment.
22. There may be circumstances where GCSB or NZSIS know or assess there is a real risk that intelligence received, including unsolicited intelligence,<sup>6</sup> was gained through a serious human rights breach. In such circumstances GCSB and NZSIS must not take action that would contribute to a further human rights breach – for example, by requesting further intelligence about the same matter from the party responsible for that breach.
23. Where GCSB or NZSIS know or assess there is a real risk that intelligence received from an overseas partner was obtained through serious human rights breaches, the agencies may only use that intelligence in exceptional circumstances. Such circumstances are where the use of the intelligence is necessary to prevent loss of life, significant personal injury or a threat to critical national infrastructure. The reasons for limiting the use of intelligence in this way are:
  - a) It is consistent with New Zealand's opposition to torture and similar mistreatment.

---

<sup>6</sup> Unsolicited intelligence is intelligence received that was not specifically requested nor otherwise sought, but was received in the course of general intelligence sharing or cooperation with foreign partners.

## UNCLASSIFIED

- b) There is a high likelihood that intelligence obtained through torture is unreliable.
24. GCSB and NZSIS do not have an enforcement function. Therefore, in such exceptional circumstances, the agencies must provide the intelligence to the relevant enforcement agency so that those agencies can take the action necessary to prevent the loss of life, significant personal injury or threat to critical national infrastructure. In these circumstances, the responsible Minister and the Inspector-General of Intelligence and Security must be informed as soon as practicable.
25. GCSB and NZSIS may still be required to undertake inquiries and investigate the intelligence that was passed to the relevant enforcement agency in order to inform the threat picture (for example, to identify the persons involved) or to provide advice to the Government on the particular security concern or risk.
26. When sharing such intelligence with law enforcement agencies, GCSB and NZSIS must mark the intelligence as having been potentially obtained as a result of torture and notify the recipient to ensure the intelligence is not used as evidence in legal proceedings.

### ***Necessity***

27. Cooperation with overseas public authorities must be for the purpose of contributing to the protection of New Zealand's national security, the international relations and well-being of New Zealand, or the economic well-being of New Zealand.
28. This may include cooperation to establish or maintain an international relationship. For example, establishing a new relationship in order to obtain intelligence relating to one (or more) of the Government's priorities may be considered necessary to enable the agencies to provide relevant intelligence and advice to the New Zealand government.

### ***Reasonableness and proportionality***

29. Cooperation with overseas public authorities, including any specific activities carried out as part of that cooperation, should be reasonable and proportionate to the purpose for carrying out that cooperation, the benefit gained from the cooperation, and the reputational risk to GCSB, NZSIS or the New Zealand Government.
30. Relevant factors in determining the reasonableness and proportionality of cooperation with an overseas public authority include:
- a) the purpose and likely outcome of the cooperation;
  - b) the volume and detail of intelligence to be shared as part of the cooperation;
  - c) the nature of the cooperation;
  - d) the appropriate or necessary protections and/or restrictions in relation to the cooperation, including protections for New Zealanders; and
  - e) the status of New Zealand's bilateral relationship with that country, including any issues or areas of sensitivity that could have a bearing on the proposed cooperation.

## UNCLASSIFIED

### ***Protections for New Zealanders***

31. When cooperating with overseas public authorities, GCSB and NZSIS must continue to apply the same protections that would normally apply in New Zealand in relation to the specific activity. GCSB and NZSIS must not cooperate with an overseas public authority for the purposes of avoiding or circumventing those protections.
32. Where cooperation with an overseas public authority involves the sharing of intelligence or personal information relating to New Zealanders, GCSB and NZSIS will have particular regard to privacy interests when determining whether to disclose that personal information to, or when requesting such information from, overseas public authorities. This includes adherence to the information privacy principles contained in Part 3 of the Privacy Act 2020 as they apply to GCSB and NZSIS.

### ***Information management***

33. GCSB and NZSIS must be satisfied that the overseas public authority has adequate protections in place for the use and storage of information, including adequate protections against on-sharing with third parties without express consent from GCSB or NZSIS. These protections will be consistent with the principles in this MPS and the MPS on *Management of information obtained by GCSB and NZSIS*. In the event of a privacy breach, including the unauthorised on-sharing of information with third parties, the agencies will act in accordance with Part 6 of the Privacy Act 2020.

### ***Oversight***

34. GCSB and NZSIS must carry out all cooperation with overseas public authorities in a manner that facilitates effective accountability, transparency and oversight, including that of the Inspector-General of Intelligence and Security. This includes:
  - appropriate record-keeping, in accordance with the Public Records Act 2005, which clearly outlines assessments and decision-making,
  - maintaining up-to-date internal policies, procedures and guidance for staff, and
  - reporting to the responsible Minister on the nature and outcomes of cooperation with overseas public authorities.
35. Reporting must include a specific section in GCSB and NZSIS annual reports on the agencies' intelligence and security relationships with overseas partners.

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

---

36. As public service agencies, GCSB and NZSIS must comply with policies and procedures common to all New Zealand public service agencies.<sup>7</sup>

---

<sup>7</sup> This includes the Public Service Act 2020 and the Health and Safety at Work Act 2015.

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

UNCLASSIFIED

37. 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 have systems in place to support and monitor compliance.

38. These policies and procedures must also address the following matters:

- ***Human rights policy***

GCSB and NZSIS must have a policy setting out the factors in the Risk Assessment Framework. These factors must be considered when assessing whether a real risk of human rights breaches may exist in connection with cooperation with overseas public authorities, whether the cooperation is one off or ongoing. This policy must also include what specific information is required to be provided to the responsible Minister to inform decision-making when seeking authorisation (either on a case-by-case basis or in the form of a broader standing authorisation) to provide intelligence or analysis to an overseas public authority.

The policy must be forwarded in draft to the Inspector-General of Intelligence and Security for comment. The final version must be referred to the Intelligence and Security Committee (ISC) for noting.

This policy is important to ensure that employees act consistently with legal obligations and the Risk Assessment Framework in this MPS.

- ***Consultation with the Ministry of Foreign Affairs and Trade***

The Ministry of Foreign Affairs and Trade is to be consulted on arrangements with foreign jurisdictions or international organisations. Foreign policy objectives should be considered in the development and framing of cooperation arrangements with foreign partners.

GCSB and NZSIS should have regard to any information available from the Ministry of Foreign Affairs and Trade on the status of the bilateral relationship with a country, a country's ratification of international human rights treaties and the human rights practices of a particular country.

- ***Written basis for new formal arrangements***

In order to support greater transparency and enable a level of Parliamentary oversight, certain newly entered arrangements<sup>8</sup> relating to cooperation with an overseas public authority, including any significant new arrangement entered into with an existing partner, or significant modification to an existing arrangement, must be referred to the ISC for noting in accordance with the considerations below. Such arrangements should be recorded in writing.

An arrangement that meets one of the following criteria must be referred to the ISC for noting:

---

<sup>8</sup> An arrangement refers to an international instrument of less-than-treaty status (that is, it is not intended to be legally binding, but can still create important political commitments). For the purposes of this MPS, treaties where there has been a treaty examination waiver issued are also to be included within this definition.

## UNCLASSIFIED

- is likely to have significant implications for New Zealand's foreign policy or international relations;
- results in a significant change to the agencies' priorities or intelligence focus;
- involves significant expenditure of funds; and / or
- is seen to be inconsistent with Government objectives or priorities.

This includes arrangements that involve other government departments where GCSB and NZSIS are acting as the lead agency/agencies to the arrangement or the arrangement creates specific roles or obligations for the agencies. If there is any doubt whether the arrangement should be referred to the ISC, the arrangement must be referred to the Chair of the ISC for decision.

- **Training**

GCSB and NZSIS employees making decisions or taking any action relating to cooperation with an overseas public authority for the purpose of performing the agencies functions must be provided training on all relevant law, policies and procedures in relation to human rights obligations. This training should be provided to existing employees and new employees, and must be updated whenever there are changes or updates to the policies and procedures to ensure that at all times employees are aware of their obligations and how to apply them in practice.

### **Duration of ministerial policy statement**

39. This MPS will take effect from 1 April 2021 for a period of three years. The Minister who issued an MPS may, at any time, amend, revoke or replace the MPS.

**Appendix One – Human Rights Information**

---

1. A request to obtain Ministerial authorisation, whether a request for a one-off or standing authorisation, must include information regarding:
  - a) the purpose of the intelligence sharing, including how it contributes to GCSB's and NZSIS's statutory objectives and functions; and
  - b) any particular risks to human rights associated with the proposed cooperation and how likely it is that breaches could occur; and
  - c) where risk is identified, the factors that mitigate the likelihood of the human rights breach occurring. Such factors might include:
    - i. the existence and effectiveness of mechanisms for monitoring or reviewing compliance with human rights obligations,
    - ii. the reliability of any assurances provided by the foreign partner about how information will be used or how information to be provided was obtained, and
    - iii. how likely the foreign partner is to comply with caveats associated with cooperation or use of information.
2. To assess the human rights practices of a country or public authority, in order to inform Ministerial authorisations and other actions by the agencies, GCSB and NZSIS should consider the following factors, as relevant:
  - a) the human rights record of the country or public authority, and any other country or public authority that may also be involved, including consideration of reports from credible international, governmental and non-governmental organisation sources;
  - b) whether the country has ratified relevant international human rights treaties, including any reservations that may have been made;
  - c) whether the country has mechanisms for independently investigating breaches of human rights;
  - d) whether the country has an independent judiciary with jurisdiction to hear cases relating to breaches of human rights;
  - e) whether the country has an established history of compliance with human rights obligations;
  - f) whether the country has an established history of investigating and prosecuting human rights breaches; and
  - g) whether the country has a legal framework and institutional arrangements that guide and appropriately constrain the activities of the country's intelligence and security sector.



## Appendix Two: New Zealand's Core Human Rights Obligations

### *Domestic law*

---

To ensure that New Zealand meets its human rights obligations, GCSB and NZSIS employees must act consistently with domestic law under (but not limited to) the following statutes:

- New Zealand Bill of Rights Act 1990
- Human Rights Act 1993
- Privacy Act 2020
- Crimes Act 1961
- Crimes of Torture Act 1989
- Geneva Conventions Act 1958
- International Crimes and International Criminal Court Act 2000

### *International Obligations*

---

New Zealand is a party to the following core international human rights instruments of the United Nations, and in doing so is bound by, and must regularly report on implementation and compliance with the obligations within those instruments. Actions or activities that run contrary to the obligations within these instruments may constitute a human rights breach in the context of this MPS.

- The International Covenant on Civil and Political Rights
- Second Optional Protocol to the International Covenant on Civil and Political Rights
- Convention Against Torture and other Cruel, Inhuman or Degrading Treatment or Punishment
- The International Covenant on Economic, Social and Cultural Rights
- The Convention on the Elimination of All Forms of Racial Discrimination
- Convention on the Rights of Persons with Disabilities
- Convention on the Elimination of all Forms of Discrimination against Women
- Convention Relating the Status of Refugees
- Convention on the Rights of the Child

New Zealand is also a party to other international criminal and international humanitarian instruments, of which the following may be relevant in the context of GCSB and NZSIS cooperating with overseas public authorities:

- Rome Statute of the International Criminal Court
- Geneva Conventions and their protocols

New Zealand may also have other relevant obligations under customary international law.

# ATTACHMENT B

## Letter to Acting Director-General of GCSB

Bridget White  
Acting Director-General  
Government Communications Security Bureau  
Pipitea House  
**WELLINGTON**

Dear Bridget

### **Ministerial Policy Statement: Cooperating with overseas public authorities**

I enclose the ministerial policy statement (MPS) I have reissued under section 207 of the Intelligence and Security Act 2017 on Cooperating with overseas public authorities. This will take effect from 1 April 2021.

There are two matters that I would like to provide additional guidance on, over and above the MPS itself:

1. s6(a)



2. s6(a)



I expect that this revised MPS will be brought to the attention of all employees of GCSB, and that all the required actions, including updating internal policies and procedures and training, will be implemented as soon as practicable. This includes revising the Joint Policy Statement on Human Rights Risk Management (JPS), which must be referred to the ISC for noting.

Yours sincerely

Hon Andrew Little

**Minister Responsible for the GCSB**

Copied to Inspector-General of Intelligence and Security

# ATTACHMENT C

## Letter to Director-General of Security

Rebecca Kitteridge  
Director-General of Security  
New Zealand Security Intelligence Service  
Pipitea House  
WELLINGTON

Dear Rebecca

### Ministerial Policy Statement: Cooperating with overseas public authorities

I enclose the ministerial policy statement (MPS) I have reissued under section 207 of the Intelligence and Security Act 2017 on Cooperating with overseas public authorities. This will take effect from 1 April 2021.

There are two matters that I would like to provide additional guidance on, over and above the MPS itself:

1. s6(a)



2. s6(a)



I expect that this revised MPS will be brought to the attention of all employees of NZSIS, and that all the required actions, including updating internal policies and procedures and training, will be implemented as soon as practicable. This includes revising the Joint Policy Statement on Human Rights Risk Management (JPS), which must be referred to the ISC for noting.

Yours sincerely

Hon Andrew Little

**Minister Responsible for the NZSIS**

Copied to Inspector-General of Intelligence and Security

# ATTACHMENT D

## Letter to Hon Kris Faafoi, Minister of Justice

Hon Kris Faafoi  
Minister of Justice  
Parliament Buildings

Dear Minister Faafoi

### **Consultation on ministerial policy statement: Cooperating with overseas public authorities**

Thank you for your recent feedback on the draft revised ministerial policy statement: Cooperating with overseas public authorities. You suggested that the ministerial policy statement be amended to *'rather than just referring to rights recognised in New Zealand law, it could more broadly refer to New Zealand law and international obligations under Treaties New Zealand has signed up to'*.

I have considered this feedback, and have sought advice from officials, but have decided not to amend the MPS. This is because:

- a) The term in the MPS *'all human rights obligations recognised by New Zealand law'* is the wording from the Intelligence and Security Act 2017 (the Act). Amending this text in the MPS would mean the MPS inconsistent with the Act;
- b) The proposed wording you have suggested is not an exhaustive list of the agencies' relevant legal obligations as, in addition to domestic law and treaties (generally implemented through domestic law), these obligations may also be sourced in customary international law and UNSC resolutions;
- c) Paragraph 13 of the MPS signals there are a range of obligations which apply to the agencies, and the core human rights obligations are set out in an Appendix to the MPS. I do not believe it is necessary to provide an exhaustive list of obligations in the body of the MPS.

Once again, I am grateful for the time you have taken to review the ministerial policy statement and appreciate your views.

Yours sincerely

Hon Andrew Little  
**Minister Responsible for the GCSB**  
**Minister Responsible for the NZSIS**



# Briefing

## CONSULTATION ON THREE MINISTERIAL POLICY STATEMENTS

To Minister Responsible for the GCSB and NZSIS (Hon Andrew Little)

Date	8/04/2021	Priority	Routine
Deadline	19/04/2021	Briefing Number	2021NSP/086

### Purpose

This briefing outlines the proposed changes to three draft Ministerial Policy Statements (MPS) following their recent review:

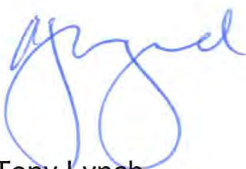
- False or misleading representations about employment;
- Legal entities; and
- Assumed identities.

It also seeks your agreement to send draft letters and revised drafts of the MPSs to relevant Ministers for consultation, as required under the Intelligence and Security Act 2017.

### Recommendations

1. **Note** that we have consulted with relevant agencies and entities on proposed revisions to three Ministerial Policy Statements;
2. **Approve** the draft revised Ministerial Policy Statement (MPS): *False or misleading representations about employment* (Attachment A) for ministerial consultation; YES / NO
3. **Sign** and forward the attached letter (Attachment C) to Hon Chris Hipkins, Minister for the Public Service, attaching the draft *False or misleading representations about employment* MPS; YES / NO
4. **Approve** the draft revised Ministerial Policy Statement (MPS): *Legal Entities* (Attachment D) for ministerial consultation; YES / NO
5. **Sign** and forward the attached letters, attaching the draft *Legal Entities* MPS, to:

- 5.1. Hon Grant Robertson, Minister of Finance (Attachment F); and YES / NO
- 5.2. Hon Jan Tinetti, Minister of Internal Affairs (Attachment G); YES / NO
- 6. **Approve** the draft revised Ministerial Policy Statement (MPS): *Assumed Identities* (Attachment H) for ministerial consultation; YES / NO
- 7. **Sign** and forward the attached letters, attaching the draft *Assumed Identities* MPS, to:
  - 7.1. Hon Poto Williams, Minister of Police (Attachment J); YES / NO
  - 7.2. Hon Jan Tinetti, Minister of Internal Affairs (Attachment K) ; and YES / NO
  - 7.3. Hon Michael Wood, Minister of Transport (Attachment L). YES / NO

  
Tony Lynch  
Deputy Chief Executive  
National Security Group

8.4.21  
...../...../.....

Hon Andrew Little  
Minister Responsible for the GCSB  
Minister Responsible for the NZSIS

...../...../.....

Contact for telephone discussion if required:

Name	Position	Telephone	1st contact
Pip Swaney	Manager, Security and Intelligence Policy, National Security Group	s9(2)(a) [REDACTED]	
Lynda Byrne	Principal Policy Advisor, Security and Intelligence Policy, National Security Group	s9(2)(a) [REDACTED]	✓

Minister's office comments:

- Noted
- Seen
- Approved
- Needs change
- Withdrawn
- Not seen by Minister
- Overtaken by events
- Referred to

# CONSULTATION ON THREE MINISTERIAL POLICY STATEMENTS

## Purpose

1. This briefing outlines the proposed changes to three draft Ministerial Policy Statements (MPS) following their recent review:
  - False or misleading representations about employment;
  - Legal entities; and
  - Assumed identities.
2. It also seeks your agreement to send draft letters and revised drafts of the MPSs to relevant Ministers for consultation, as required under the Intelligence and Security Act 2017 (the Act).

## DPMC is reviewing the MPSs on your behalf

3. Under the Act the MPSs are required to be reissued every three years. The Department of the Prime Minister and Cabinet, working closely with GCSB and NZSIS, is reviewing the MPSs on your behalf.
4. The following table provides an update up where the review is up to in relation to each of the MPSs. We expect all MPSs to be reissued in mid-2021.

MPS	Status
1. Overseas cooperation	Reissued on 1 April 2021
2. Road user rules exemption	Ministerial consultation completed, will reissue when other MPSs reviewed
3. Conducting surveillance in a public place	Ministerial consultation completed, will reissue when other MPSs reviewed
4. False and misleading representations about employment	Attached
5. Legal entities	Attached
6. Assumed identities	Attached
7. Information management	Out for cross-agency consultation
8. Human intelligence	In final stages of review
9. Requesting information from agencies	In final stages of review
10. Publicly available information	In final stages of review
11. Information assurance and cybersecurity activities	In final stages of review



## How did we review the three attached MPSs?

---

5. To review these MPSs we worked with GCSB and NZSIS on whether the MPS provided clear and appropriate guidance to agencies on the activity covered by the MPS. We looked at how the agencies had incorporated the MPS into their operations and whether there were any problems with the MPS. Descriptions of each MPS and the consultation undertaken during the review are set out below.

### *False or misleading representations about employment*

6. The false or misleading representations about employment MPS sets out your expectations, as the responsible Minister, for how GCSB and NZSIS properly make false or misleading representations about their employment.
7. To review the false and misleading representations MPS, we consulted with:
- The Inspector-General of Intelligence and Security;
  - Te Kawa Mataaho Public Service Commission, to consider the broader public sector interests when employees of one agency purport to be employed by another agency; and
  - Other relevant government agencies.

### *Legal entities*

8. The Legal Entities MPS sets out your expectations, as the responsible Minister, for how GCSB and NZSIS properly create and maintain a legal entity. Any agency that receives a request for assistance to create or maintain a legal entity must also have regard to the MPS.
9. In reviewing this MPS, we consulted with:
- The Inspector-General of Intelligence and Security;
  - The Department of Internal Affairs – as an agency who receives requests for assistance in creating a legal entity;
  - The Ministry of Business, Innovation and Employment – as an agency who receives requests for assistance in creating a legal entity and to ensure the MPS complies with the whole-of-government procurement requirements; and
  - The Treasury – to ensure the MPS complies with the obligations under the Public Finance Act 1989.

### *Assumed identities*

10. The Assumed Identities MPS sets out your expectations, as the responsible Minister, for how GCSB and NZSIS properly acquire, maintain and use an assumed identity. Agencies, public or private, that receive requests for assistance regarding assumed identities also must also have regard to this MPS.
11. We consulted with:
- The Inspector-General of Intelligence and Security;

- NZ Police – as an operational agency that undertakes similar activities;
  - The Department of Internal Affairs – as an agency that receives requests for assistance to acquire an assumed identity; and
  - The Ministry of Transport and Waka Kotahi – as agencies that also receive requests for assistance to acquire an assumed identity.
12. The Assumed Identity and Legal Entity MPSs were reviewed together as they cover similar activities.

## Proposed changes to the MPSs

---

13. The feedback on the three MPSs was that they generally provided appropriate guidance to the agencies, but they could be made clearer and more succinct. As a result, we propose the following changes:
- Restructuring and streamlining the MPSs to make them easier to read, including:
    - shortening the titles;
    - developing a common 'cover-sheet' that sets out the overarching purpose of all MPSs which, once all MPSs are reissued will become the 'landing page' for the website versions of all the MPSs;
    - simplifying the language used;
    - reducing repetition;
    - reworking them to better align with the Act;
    - aligning the Assumed Identities and Legal Entities MPSs.
14. Our understanding is that there are no outstanding matters of disagreement with the GCSB, NZSIS or other agencies that were consulted on these MPSs.
15. The revised MPSs are attached, for you to consult with relevant Ministerial colleagues as you are required to do under the Act. We have proposed relevant Ministers on the basis that the agencies for which they are responsible were consulted on the revised MPSs, as reflected in the attached draft letters. The Ministers we recommend consulting with are:

### *False and misleading representations*

- Hon Chris Hipkins, Minister for the Public Service,

### *Legal entities*

- Hon Grant Robertson, Minister of Finance;
- Hon Jan Tinetti, Minister of Internal Affairs;

### *Assumed Identities*

- Hon Poto Williams, Minister of Police
- Hon Jan Tinetti, Minister of Internal Affairs; and

- Hon Michael Wood, Minister of Transport.

16. We have also provided the 2017 versions for your information.

## Next Steps

17. If you agree with the proposed revised MPSs as attached, we recommend you sign the attached letters to send to your ministerial colleagues, as required under the Act.
18. Once you receive any feedback from your consultation, we can adapt the MPSs to reflect any comments if you wish. Subject to your final decision, the MPSs can then be finalised and reissued in mid-2021 once the remainder of the MPSs have been reviewed.

Attachments:		
<b>Attachment A:</b>	Unclassified	<b>Draft revised Ministerial Policy Statement: <i>False or misleading representations about employment</i></b>
<b>Attachment B:</b>	Unclassified	2017 version of Ministerial Policy Statement: <i>Making false or misleading representations under section 228 of the Intelligence and Security Act 2017 about being employed with an intelligence and security agency</i>
<b>Attachment C:</b>	Unclassified	Letter to Hon Chris Hipkins, Minister for the Public Service
<b>Attachment D:</b>	Unclassified	<b>Draft revised Ministerial Policy Statement: <i>Legal Entities</i></b>
<b>Attachment E:</b>	Unclassified	2017 version of Ministerial Policy Statement: <i>Creating and maintaining a legal entity under subpart 2 of Part 3 of the Intelligence and Security Act 2017</i>
<b>Attachment F:</b>	Unclassified	Letter to Hon Grant Robertson, Minister of Finance
<b>Attachment G:</b>	Unclassified	Letter to Hon Jan Tinetti, Minister of Internal Affairs
<b>Attachment H:</b>	Unclassified	<b>Draft revised Ministerial Policy Statement: <i>Assumed Identities</i></b>
<b>Attachment I:</b>	Unclassified	2017 version of Ministerial Policy Statement: <i>Creating, using and maintaining an assumed identity under subpart 1 of Part 3 of the Intelligence and Security Act 2017</i>
<b>Attachment J:</b>	Unclassified	Letter to Hon Poto Williams, Minister of Police
<b>Attachment K:</b>	Unclassified	Letter to Hon Jan Tinetti, Minister of Internal Affairs
<b>Attachment L:</b>	Unclassified	Letter to Hon Michael Wood, Minister of Transport

**ATTACHMENT A**

**Draft revised Ministerial Policy Statement: false or misleading representations about employment**

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

**ATTACHMENT B**

**2017 version of Ministerial Policy Statement: Making false or misleading representations under section 228 of the Intelligence and Security Act 2017 about being employed with an intelligence and security agency**

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

## ATTACHMENT C

### Letter to Hon Chris Hipkins, Minister for the Public Service

Hon Chris Hipkins  
Minister for the Public Service  
Parliament Buildings

Dear Minister Hipkins

#### **Consultation on Ministerial Policy Statement – False or misleading representations about employment**

I enclose for your comment a draft of the revised Ministerial Policy Statement (MPS) regarding GCSB and NZSIS making false or misleading representations about employment.

Sections 206 and 207 of the Intelligence and Security Act (the Act) requires the Minister(s) responsible for the intelligence and security agencies to issue MPSs about certain lawful activities carried out by the agencies. The MPSs are required to be reviewed within three years from the date they take effect.

MPSs are a mechanism for the responsible Minister(s) to set expectations and provide guidance about the conduct of those activities. MPSs do not affect the lawfulness of the activities, but may be taken into account by the Inspector-General of Intelligence and Security when they are assessing the propriety of the agencies' activities. As the current Minister responsible for both the GCSB and the NZSIS, I must review and reissue the MPSs.

Under section 212 of the Act I am required to consult with any Ministers of the Crown whose area of responsibility includes an interest in the proposed statement. In this case, I seek your comments as the MPS is relevant to your portfolio responsibilities as Minister for the Public Service.

If you have any comments, I would be grateful to receive these by **[date]**.

Given your portfolio responsibilities for the Public Service, I would welcome any insights that you may have, particularly to ensure the MPS captures the broader public sector interests that come into play when employees of one agency purport to be employed by another agency. Officials from the Department of the Prime Minister and Cabinet have liaised with officials from Te Kawa Mataaho Public Service Commission and their feedback has been incorporated in the attached draft.

Yours sincerely

Hon Andrew Little  
**Minister Responsible for the GCSB**  
**Minister Responsible for the NZSIS**

UNCLASSIFIED

## ATTACHMENT D

Draft revised Ministerial Policy Statement: Legal Entities

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

UNCLASSIFIED

## ATTACHMENT E

2017 version of Ministerial Policy Statement: Creating and maintaining a legal entity under subpart 2 of Part 3 of the Intelligence and Security Act 2017

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982



## ATTACHMENT F

### Letter to Hon Grant Robertson, Minister of Finance

Hon Grant Robertson  
Minister of Finance  
Parliament Buildings

Dear Minister Robertson

#### **Consultation on Ministerial Policy Statement – Legal Entities**

I enclose for your comment a draft of the revised Ministerial Policy Statement (MPS) regarding GCSB and NZSIS creating and maintaining legal entities.

Sections 206 and 207 of the Intelligence and Security Act (the Act) requires the Minister(s) responsible for the intelligence and security agencies to issue MPSs about certain lawful activities carried out by the agencies. The MPSs are required to be reviewed within three years from the date they take effect.

MPSs are a mechanism for the responsible Minister(s) to set expectations and provide guidance about the conduct of those activities. MPSs do not affect the lawfulness of the activities, but may be taken into account by the Inspector-General of Intelligence and Security when they are assessing the propriety of the agencies' activities. As the Minister responsible for both the GCSB and the NZSIS, I must review and reissue the MPSs.

Under section 212 of the Act I am required to consult with any Ministers of the Crown whose area of responsibility includes an interest in the proposed statement. In this case, I seek your comments as the MPS is relevant to your portfolio responsibilities as Minister of Finance.

If you have any comments, I would be grateful to receive these by **[date]**.

Given your portfolio responsibilities for Government's fiscal policy and the Public Finance Act 1989, I welcome any insights you may have. Officials from the Department of the Prime Minister and Cabinet have liaised officials from the Treasury and the Ministry of Business, Innovation and Employment and their feedback has been incorporated in the attached draft.

Yours sincerely

Hon Andrew Little  
**Minister Responsible for the GCSB**  
**Minister Responsible for the NZSIS**

## ATTACHMENT G

### Letter to Hon Jan Tinetti, Minister of Internal Affairs

Hon Jan Tinetti  
Minister of Internal Affairs  
Parliament Buildings

Dear Minister Tinetti

#### **Consultation on Ministerial Policy Statement – Legal Entities**

I enclose for your comment a draft of the revised Ministerial Policy Statement (MPS) regarding GCSB and NZSIS creating and maintaining legal entities.

Sections 206 and 207 of the Intelligence and Security Act (the Act) requires the Minister(s) responsible for the intelligence and security agencies to issue MPSs about certain lawful activities carried out by the agencies. The MPSs are required to be reviewed within three years from the date they take effect.

MPSs are a mechanism for the responsible Minister(s) to set expectations and provide guidance about the conduct of those activities. MPSs do not affect the lawfulness of the activities, but may be taken into account by the Inspector-General of Intelligence and Security when they are assessing the propriety of the agencies' activities. As the Minister responsible for both the GCSB and the NZSIS, I must review and reissue the MPSs.

Under section 212 of the Act I am required to consult with any Ministers of the Crown whose area of responsibility includes an interest in the proposed statement. In this case, I seek your comments as the MPS is relevant to your portfolio responsibilities as Minister of Internal Affairs.

If you have any comments, I would be grateful to receive these by **[date]**.

Given your portfolio responsibilities for the Department of Internal Affairs, who receives requests for assistance to acquire legal entities, I am interested in any insights you may have. Officials from the Department of the Prime Minister and Cabinet have liaised officials from the Department of Internal Affairs and their feedback has been incorporated in the attached draft.

Yours sincerely

Hon Andrew Little  
**Minister Responsible for the GCSB**  
**Minister Responsible for the NZSIS**

UNCLASSIFIED

## ATTACHMENT H

Draft revised Ministerial Policy Statement: Assumed Identities

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

UNCLASSIFIED

**ATTACHMENT I**

**2017 version of Ministerial Policy Statement: Obtaining, using and maintaining an assumed identity under subpart 1 of Part 3 of the Intelligence and Security Act 2017**

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

## ATTACHMENT J

### Letter to Hon Poto Williams, Minister of Police

Hon Poto Williams  
Minister of Police  
Parliament Buildings

Dear Minister Williams

#### **Consultation on Ministerial Policy Statement – Assumed Identities**

I enclose for your comment a draft of the revised Ministerial Policy Statement (MPS) regarding GCSB and NZSIS acquiring, using and maintaining assumed identities.

Sections 206 and 207 of the Intelligence and Security Act (the Act) requires the Minister(s) responsible for the intelligence and security agencies to issue MPSs about certain lawful activities carried out by the agencies. The MPSs are required to be reviewed within three years from the date they take effect.

MPSs are a mechanism for the responsible Minister(s) to set expectations and provide guidance about the conduct of those activities. MPSs do not affect the lawfulness of the activities, but may be taken into account by the Inspector-General of Intelligence and Security when they are assessing the propriety of the agencies' activities. As the current Minister responsible for both the GCSB and the NZSIS, I must review and reissue the MPSs.

Under section 212 of the Act I am required to consult with any Ministers of the Crown whose area of responsibility includes an interest in the proposed statement. In this case, I seek your comments as the MPS is relevant to your portfolio responsibilities as Minister of Police.

If you have any comments, I would be grateful to receive these by **[date]**.

Given your portfolio responsibilities for New Zealand Police, who undertake similar activities, I would welcome any insights that you may have. Officials from the Department of the Prime Minister and Cabinet have liaised with officials from New Zealand Police and their feedback has been incorporated in the attached draft.

Yours sincerely

Hon Andrew Little  
**Minister Responsible for the GCSB**  
**Minister Responsible for the NZSIS**

## ATTACHMENT K

### Letter to Hon Jan Tinetti, Minister of Internal Affairs

Hon Jan Tinetti  
Minister of Internal Affairs  
Parliament Buildings

Dear Minister Tinetti

#### Consultation on Ministerial Policy Statement – Assumed Identities

I enclose for your comment a draft of the revised Ministerial Policy Statement (MPS) regarding GCSB and NZSIS acquiring, using and maintaining assumed identities.

Sections 206 and 207 of the Intelligence and Security Act (the Act) requires the Minister(s) responsible for the intelligence and security agencies to issue MPSs about certain lawful activities carried out by the agencies. The MPSs are required to be reviewed within three years from the date they take effect.

MPSs are a mechanism for the responsible Minister(s) to set expectations and provide guidance about the conduct of those activities. MPSs do not affect the lawfulness of the activities, but may be taken into account by the Inspector-General of Intelligence and Security when they are assessing the propriety of the agencies' activities. As the current Minister responsible for both the GCSB and the NZSIS, I must review and reissue the MPSs.

Under section 212 of the Act I am required to consult with any Ministers of the Crown whose area of responsibility includes an interest in the proposed statement. In this case, I seek your comments as the MPS is relevant to your portfolio responsibilities as Minister of Internal Affairs.

If you have any comments, I would be grateful to receive these by **[date]**.

Given your portfolio responsibilities for the Department of Internal Affairs, who receives requests for assistance to acquire assume identities, I am interested in any insights you may have. Officials from the Department of the Prime Minister and Cabinet have liaised with officials from the Department of Internal Affairs and their feedback has been incorporated in the attached draft.

Yours sincerely

Hon Andrew Little  
**Minister Responsible for the GCSB**  
**Minister Responsible for the NZSIS**

## ATTACHMENT L

### Letter to Hon Michael Wood, Minister of Transport

Hon Michael Wood  
Minister of Transport  
Parliament Buildings

Dear Minister Wood

#### **Consultation on Ministerial Policy Statement – Assumed Identities**

I enclose for your comment a draft of the revised Ministerial Policy Statement (MPS) regarding GCSB and NZSIS acquiring, using and maintaining assumed identities.

Sections 206 and 207 of the Intelligence and Security Act (the Act) requires the Minister(s) responsible for the intelligence and security agencies to issue MPSs about certain lawful activities carried out by the agencies. The MPSs are required to be reviewed within three years from the date they take effect.

MPSs are a mechanism for the responsible Minister(s) to set expectations and provide guidance about the conduct of those activities. MPSs do not affect the lawfulness of the activities, but may be taken into account by the Inspector-General of Intelligence and Security when they are assessing the propriety of the agencies' activities. As the current Minister responsible for both the GCSB and the NZSIS, I must review and reissue the MPSs.

Under section 212 of the Act I am required to consult with any Ministers of the Crown whose area of responsibility includes an interest in the proposed statement. In this case, I seek your comments as the MPS is relevant to your portfolio responsibilities as Minister of Transport.

If you have any comments, I would be grateful to receive these by **[date]**.

Given your portfolio responsibilities for the Ministry of Transport and Waka Kotahi, who receive requests for assistance to acquire assumed identities, I welcome any insights that you may have. Officials from the Department of the Prime Minister and Cabinet have liaised with officials from the Ministry of Transport and Waka Kotahi and their feedback has been incorporated in the attached draft.

Yours sincerely

Hon Andrew Little  
**Minister Responsible for the GCSB**  
**Minister Responsible for the NZSIS**

# Briefing

## CONSULTATION ON MINISTERIAL POLICY STATEMENT: INFORMATION ASSURANCE AND CYBERSECURITY ACTIVITIES

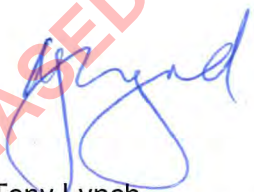
To Hon Andrew Little, Minister Responsible for the GCSB and NZSIS			
Date	2/07/2021	Priority	Routine
Deadline	23/07/2021	Briefing Number	2021NSP/111

### Purpose

This briefing outlines the proposed changes to the draft Ministerial Policy Statement (MPS): Information assurance and cybersecurity activities, as a result of agency consultation on the MPS. To support the ministerial consultation that you are required to do, it also attaches draft letters and a revised draft of the MPS for forwarding to Hon Dr David Clark, Minister for the Digital Economy and Communications.

### Recommendations

- Note** that the Department of the Prime Minister and Cabinet is reviewing the ministerial policy statements (MPSs) under the Intelligence and Security Act 2017 (the Act) on your behalf;
- Note** that we propose minor changes to the MPS: Information assurance and cybersecurity activities;
- Note** that under the Act you are required to consult relevant Ministers as the MPSs are reviewed and reissued;
- Sign** and forward the attached letter and draft revised MPS to **YES / NO** Hon Dr David Clark, Minister for the Digital Economy and Communications.

  
 Tony Lynch  
 Deputy Chief Executive  
 National Security Group

1.07.21  
 ...../...../.....

Hon Minister Andrew Little  
 Minister Responsible for the GCSB  
 Minister Responsible for the NZSIS

...../...../.....



Contact for telephone discussion if required:

Name	Position	Telephone	1st contact
Pip Swaney	Manager, Security and Intelligence Policy, National Security Group	s9(2)(a)	
Lynda Byrne	Principal Policy Advisor, Security and Intelligence Policy	s9(2)(a)	✓

Minister's office comments:

- Noted
- Seen
- Approved
- Needs change
- Withdrawn
- Not seen by Minister
- Overtaken by events
- Referred to

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

# **CONSULTATION ON MINISTERIAL POLICY STATEMENT: INFORMATION ASSURANCE AND CYBERSECURITY ACTIVITIES**

## **Purpose**

---

1. This briefing outlines the proposed changes to the draft Ministerial Policy Statement (MPS): Information assurance and cybersecurity activities, following its recent review.
2. To support the ministerial consultation that you are required to do under the Intelligence and Security Act 2017 (the Act), it also attaches a draft letter and revised draft MPS for forwarding to Hon Dr David Clark, Minister for the Digital Economy and Communications.

## **DPMC is reviewing the ministerial policy statements on your behalf**

---

3. Under the Act the MPSs are required to be reviewed within three years from the date they are issued. The Department of the Prime Minister and Cabinet is undertaking the review of the MPSs on your behalf.

## **We propose minor changes to the Information assurance and cyber security MPS**

---

4. This MPS provides guidance to the Government Communications Security Bureau (GCSB) on providing information and cybersecurity activities with consent. To review this MPS we worked with GCSB on whether the MPS provided clear and appropriate guidance to the GCSB on these activities. We also consulted with the Inspector-General of Intelligence and Security and the National Cyber Policy Office.
5. Feedback from the consultation was that on the whole, the Information assurance and cybersecurity activities MPS provided sufficient guidance to the GCSB and did not need substantive changes. The proposed changes to the MPS are to align with the GCSB website and the other MPSs, and to improve clarity and brevity. As with the other MPSs the common content has been moved into the cover-sheet, which is intended to become the MPS 'landing page' when on the NZIC website.
6. The draft revised MPS is attached at Attachment A.

## **The Act requires you to consult with relevant Ministers before reissuing the revised MPS**

---

7. The Act requires you to consult with any other Minister of the Crown whose area of responsibility includes an interest in the proposed MPS.
8. We recommend you consult with the Minister for the Digital Economy and Communications on this revised MPS. A draft letter is attached at Attachment C, for your signature.

## Next Steps

---

9. Once you have received feedback from Minister Clark, we will support you in adapting the MPS to reflect any comments, if you wish.
10. You have three MPSs with you, awaiting Ministerial consultation: Legal Entities, Assumed Identities and False and misleading representations about employment. We expect to provide you with the remaining four MPSs within the coming weeks for consultation with your ministerial colleagues, with the aim of all being reissued by August 2021.
11. When all 11 MPSs have been reviewed, we will submit them together for your signature so they can all be reissued on the same date.

Attachments:		
<b>Attachment A:</b>	Unclassified	Draft revised Ministerial Policy Statement
<b>Attachment B:</b>	Unclassified	2017 version of the Ministerial Policy Statement
<b>Attachment C:</b>	Unclassified	Draft letter to Hon Dr Clark, Minister for the Digital Economy and Communications

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

## Attachment A

---

Draft revised ministerial policy statement: *Information assurance and cybersecurity activities*

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

## Attachment B

---

**2017 ministerial policy statement: *Providing information assurance and cybersecurity activities under section 11 of the Intelligence and Security Act 2017 with consent***

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

## Attachment C

---

### Letter to Hon Dr David Clark

Hon Dr David Clark  
Minister for the Digital Economy and Communications  
Parliament Buildings

Dear Minister Clark

#### **Consultation on Ministerial Policy Statement – Information assurance and cybersecurity activities**

I enclose for your comment the draft revised ministerial policy statement (MPS) on information assurance and cyber security activities).

Sections 206 and 207 of the Act require the Minister(s) responsible for the intelligence and security agencies to issue MPSs about certain lawful activities carried out by the Government Communications Security Bureau and the New Zealand Security Intelligence Service. The MPSs are required to be reviewed within three years from the date they take effect.

MPSs are a mechanism for the responsible Minister(s) to set expectations and provide guidance about the conduct of those activities. MPSs do not affect the lawfulness of the activities, but may be taken into account by the Inspector-General of Intelligence and Security when assessing the propriety of the agencies' activities. As the current Minister for the GCSB and the NZSIS, I am responsible for reviewing and reissuing the MPSs.

Under section 212 of the Act I am required to consult with any Ministers of the Crown whose area of responsibility includes an interest in the proposed statement. In this case, I seek your comments as the Information assurance and cybersecurity activities MPS is relevant to your portfolio responsibilities as Minister for the Digital Economy and Communications.

The Department of the Prime Minister and Cabinet (DPMC) is undertaking a review of the MPSs on my behalf. In relation to this particular MPS, in addition to the GCSB, DPMC has consulted with the Inspector-General of Intelligence and Security, and the National Cyber Policy Office in DPMC. This consultation has shown that the MPS provides sufficient guidance to the GCSB and does not require substantive change. The proposed changes are to update the MPS to be consistent with the GCSB website and to improve clarity and brevity.

If you have any comments, I would be grateful to receive these by **[date]**.

Yours sincerely

Hon Andrew Little  
Minister Responsible for the GCSB  
Minister Responsible for the NZSIS

**Attachments:** Draft revised Ministerial Policy Statement: *Information assurance and cybersecurity activities*

2017 version of Ministerial Policy Statement: *Providing information assurance and cybersecurity activities under section 11 of the Intelligence and Security Act 2017 with consent*



# Briefing

## CONSULTATION ON MINISTERIAL POLICY STATEMENT: INFORMATION MANAGEMENT

To Hon Andrew Little, Minister Responsible for the GCSB and NZSIS

Date	5/07/2021	Priority	Routine
Deadline	16/07/2021	Briefing Number	2021NSP/129

### Purpose

This briefing outlines a series of proposed changes to the Ministerial Policy Statement (MPS) on Information Management, as a result of agency consultation on the MPS.

To support the Ministerial consultation that you are required to do, it also attaches draft letters and the revised draft MPS for forwarding to relevant ministers.

### Recommendations

1. **Note** that the Department of the Prime Minister and Cabinet is reviewing the ministerial policy statements (MPSs) under the Intelligence and Security Act 2017 (the Act) on your behalf;
2. **Note** that we propose a number of changes to the MPS: Information Management;
3. **Note** that under the Act you are required to consult relevant Ministers as the MPSs are reviewed and reissued;

4. **Sign** and forward the attached letters and draft MPS to:

4.1 Hon Jan Tinetti, Minister of Internal Affairs

YES / NO

4.2 Hon Kris Faafoi, Minister of Justice

YES / NO

 Tony Lynch Deputy Chief Executive National Security Group
05/07/21 ...../...../.....

Hon Andrew Little Minister Responsible for the GCSB Minister Responsible for the NZSIS
...../...../.....

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982



Contact for telephone discussion if required:

Name	Position	Telephone	1st contact
Pip Swaney	Manager, Security and Intelligence Policy, National Security Group	s9(2)(a)	
Lynda Byrne	Principal Policy Advisor, Security and Intelligence Policy	s9(2)(a)	✓
Greg Mitchell-Kouttab	Principal Policy Advisor, Security and Intelligence Policy	s9(2)(a)	

Minister's office comments:

- Noted
- Seen
- Approved
- Needs change
- Withdrawn
- Not seen by Minister
- Overtaken by events
- Referred to

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

# CONSULTATION ON MINISTERIAL POLICY STATEMENT: INFORMATION MANAGEMENT

## Purpose

---

1. This briefing outlines the proposed changes to the draft Ministerial Policy Statement (MPS): Information Management, following its recent review.
2. To support the ministerial consultation that you are required to do under the Intelligence and Security Act 2017 (the Act), it also attaches draft letters and a revised draft of the MPS for forwarding to relevant ministers.

## DPMC is reviewing the ministerial policy statements on your behalf

---

3. Under the Act the MPSs are required to be reviewed within three years from the date they are issued. The Department of the Prime Minister and Cabinet is undertaking the review of the MPSs on your behalf.

## We propose a number of changes to the Information Management MPS

---

4. This MPS provides guidance for employees on the management of information, including its retention and disposal. To review this MPS we worked with the NZSIS and GCSB on whether the MPS provided clear and appropriate guidance on managing information. We also consulted with the Inspector-General of Intelligence and Security, the Office of the Chief Archivist and the Office of the Privacy Commissioner.
5. Feedback from the consultation was that the MPS was too long and contained too much information directly taken from the Act. As a result, we propose the following changes to improve clarity and brevity:
  - a) We removed unnecessary language, including:
    - i) language directly replicated from the Act;
    - ii) definitions that are common to all MPSs, which will now be covered in a common 'landing page' for all MPSs on the NZIC website; and
    - iii) sections common to all of the information MPSs, which will now be covered in a common cover sheet for those MPSs;
  - b) We provided updates relating to the Privacy Act 2020;
  - c) We inserted advice from the Chief Archivist to give greater clarity around archives requirements;
  - d) We ensured greater clarity around requirements for the sharing and disposal of information;

- e) We made more explicit reference to the IGIS oversight role and the need for agencies to support that role; and
  - f) We provided greater detail around the necessity and proportionality requirements of information management.
6. The revised draft MPS is attached at **Attachment A**. The 2017 version of the MPS is also attached at **Attachment B**.
7. Because MPSs can only clarify current legislation, the revised draft MPS does not address information management issues raised in the report of the Royal Commission of Inquiry into the terrorist attack on Christchurch masjidain. These issues will be addressed through the statutory review of the Act, which is due to commence this year.

### The Act requires you to consult with relevant Ministers before reissuing the revised MPS

---

8. The Act requires you to consult with any other Minister of the Crown whose area of responsibility includes an interest in the proposed MPS.
9. We recommend you consult with:
- a) Hon Jan Tinetti – Minister of Internal Affairs (responsible for Archives); and
  - b) Hon Kris Faafoi – Minister of Justice (responsible for the Privacy Act 2020).
10. Draft letters to these Ministers are attached as Attachments D and E for your signature.

### Next Steps

---

11. Once you receive any feedback on the MPS from Ministerial consultation, we will support you in adapting the MPS to reflect the comments.
12. When all 11 MPSs have been reviewed, we will submit them together for your signature so they are all reissued on the same date.

Attachments:		
<b>Attachment A:</b>	Unclassified	Draft revised Ministerial Policy Statement
<b>Attachment B:</b>	Unclassified	Common MPS landing page
<b>Attachment C:</b>	Unclassified	2017 version of the Ministerial Policy Statement
<b>Attachment D:</b>	Unclassified	Draft letter to Hon Jan Tinetti, Minister of Internal Affairs
<b>Attachment E:</b>	Unclassified	Draft letter to Hon Kris Faafoi, Minister of Justice

## Attachment A

---

Draft revised Ministerial Policy Statement: Information Management

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

**Attachment B**

---

**Common MPS landing page**

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

## Attachment C

---

2017 version of Ministerial Policy Statement: The management of information obtained by GCSB and NZSIS, including retention and disposal of that information

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

## Attachment D

---

**Hon Jan Tinetti**  
**Minister of Internal Affairs**  
Parliament Buildings

Dear Minister Tinetti

### **Consultation on Ministerial Policy Statement: Information Management**

I enclose for your comment the draft revised ministerial policy statement (MPS) on Information Management.

Sections 206 and 207 of the Act require the Minister(s) responsible for the intelligence and security agencies to issue MPSs about certain lawful activities carried out by the Government Communications Security Bureau and the New Zealand Security Intelligence Service. The MPSs are required to be reviewed within three years from the date they take effect.

MPSs are a mechanism for the responsible Minister(s) to set expectations and provide guidance about the conduct of those activities. MPSs do not affect the lawfulness of the activities, but may be taken into account by the Inspector-General of Intelligence and Security when they are assessing the propriety of the agencies' activities. As the current Minister for the GCSB and the NZSIS, I am responsible for reviewing and reissuing the MPSs.

Under section 212 of the Act I am required to consult with any Ministers of the Crown whose area of responsibility includes an interest in the proposed statement. In this case, I seek your comments as the MPS has relevance to your portfolio responsibilities as Minister of Internal Affairs (with responsibility for Archives).

The Department of the Prime Minister and Cabinet is undertaking a review of the MPSs on my behalf. In relation to this particular MPS, in addition to the NZSIS and GCSB, DPMC has consulted with the Inspector-General of Intelligence and Security, the Office of the Chief Archivist and the Office of the Privacy Commissioner. The consultation highlighted that a number of changes were required to this MPS to provide greater clarity and brevity, and to reflect the new Privacy Act 2020.

If you have any comments, I would be grateful to receive these by **[date]**.

Yours sincerely

Hon Andrew Little  
**Minister Responsible for the GCSB**  
**Minister Responsible for the NZSIS**

**Attachments:** Draft revised Ministerial Policy Statement: Information Management

2017 version of Ministerial Policy Statement: Information Management: *The management of information obtained by GCSB and NZSIS, including retention and disposal of that information*

## Attachment E

---

Hon Kris Faafoi  
Minister of Justice  
Parliament Buildings

Dear Minister Faafoi

### Consultation on Ministerial Policy Statement: Information Management

I enclose for your comment the draft revised ministerial policy statement (MPS) on Information Management.

Sections 206 and 207 of the Act require the Minister(s) responsible for the intelligence and security agencies to issue MPSs about certain lawful activities carried out by the Government Communications Security Bureau and the New Zealand Security Intelligence Service. The MPSs are required to be reviewed within three years from the date they take effect.

MPSs are a mechanism for the responsible Minister(s) to set expectations and provide guidance about the conduct of those activities. MPSs do not affect the lawfulness of the activities, but may be taken into account by the Inspector-General of Intelligence and Security when they are assessing the propriety of the agencies' activities. As the current Minister for the GCSB and the NZSIS, I am responsible for reviewing and reissuing the MPSs.

Under section 212 of the Act I am required to consult with any Ministers of the Crown whose area of responsibility includes an interest in the proposed statement. In this case, I seek your comments as the MPS has relevance to your portfolio responsibilities as Minister of Justice (with responsibility for the Privacy Act 2020).

The Department of the Prime Minister and Cabinet is undertaking a review of the MPSs on my behalf. In relation to this particular MPS, in addition to the NZSIS and GCSB, DPMC has consulted with the Inspector-General of Intelligence and Security, the Office of the Chief Archivist and the Office of the Privacy Commissioner. The consultation highlighted that a number of changes were required to this MPS to provide greater clarity and brevity, and to reflect the new Privacy Act 2020.

If you have any comments, I would be grateful to receive these by **[date]**.

Yours sincerely

Hon Andrew Little  
Minister Responsible for the GCSB  
Minister Responsible for the NZSIS

**Attachments:** Draft revised Ministerial Policy Statement: Information Management

2017 version of Ministerial Policy Statement: Information Management: *The management of information obtained by GCSB and NZSIS, including retention and disposal of that information*





# Briefing

## CONSULTATION ON THE FINAL THREE REVIEWED MINISTERIAL POLICY STATEMENTS

To Minister Responsible for the GCSB and NZSIS (Hon Andrew Little)

Date	27/10/2021	Priority	Routine
Deadline	5/11/2021	Briefing Number	2122NSP/050

### Purpose

This briefing outlines the proposed changes to the final three Ministerial Policy Statements (MPS) that have been reviewed:


- Collecting human intelligence;
- Publicly available information; and
- Section 121 requests.

It also seeks your agreement to send draft letters and revised drafts of the MPSs to relevant Ministers for consultation, as required under the Intelligence and Security Act 2017.

### Recommendations

1. **Note** that we have consulted with relevant agencies on all three revised MPSs;
2. **Approve** the draft revised MPS: *Collecting Human Intelligence* (Attachment A) for Ministerial consultation; YES / NO
3. **Approve** the draft revised MPS: *Publicly available information* (Attachment C) for Ministerial consultation; YES / NO
4. **Approve** the draft revised MPS: *Section 121 Requests* (Attachment E) for Ministerial consultation; YES / NO
5. **Sign** and forward the attached letter (Attachment G) to Hon Kris Faafoi, Minister of Justice, attaching the draft *Publicly Available Information MPS*; YES / NO

- 6. **Sign** and forward the attached letter (Attachment G) to Hon Dr David Clark, Minister for Digital Economy and Communications, attaching the draft Publicly Available Information MPS; YES / NO
- 7. **Sign** and forward the attached letter (Attachment H) to Hon Poto Williams, Minister of Police, attaching the three draft MPSs. YES / NO

 Tony Lynch Deputy Chief Executive National Security Group
27, 10 ...../...../2021

    Hon Andrew Little Minister Responsible for the GCSB Minister Responsible for the NZSIS
...../...../2021

Contact for telephone discussion if required:

Name	Position	Telephone	1st contact
Pip Swaney	Manager, Security and Intelligence Policy, National Security Group	s9(2)(a)	
Lynda Byrne	Principal Policy Advisor, Security and Intelligence Policy, National Security Group	s9(2)(a)	✓

Minister's office comments:

- Noted
- Seen
- Approved
- Needs change
- Withdrawn
- Not seen by Minister
- Overtaken by events
- Referred to

# CONSULTATION ON THE FINAL THREE MINISTERIAL POLICY STATEMENTS

## Purpose

---

1. This briefing outlines the proposed changes to the final three Ministerial Policy Statements (MPSs) that have been reviewed:
  - Collecting human intelligence;
  - Publicly available information; and
  - Section 121 requests.
2. It also seeks your agreement to send draft letters and revised drafts of the MPSs to relevant Ministers for consultation, as required under the Intelligence and Security Act 2017.

## These are the final MPSs to be reviewed

---

3. The Department of the Prime Minister and Cabinet, working closely with GCSB and NZSIS, is reviewing the eleven MPSs on your behalf. The Overseas Cooperation MPS was reviewed and reissued on 1 April 2021. All other MPS have been reviewed and can be reissued together once the attached MPSs have been consulted with relevant Ministers, and any revisions made.

## How did we review these MPSs?

4. We reviewed the Collecting Human Intelligence, Publicly Available Information and Section 121 MPSs at the same time, as they all relate to information collection. We worked with the policy, legal and operational branches of the GCSB and NZSIS to consider:
  - a) whether the MPS provided clear and appropriate guidance to the agencies on the activity covered by the MPS;
  - b) how the agencies had incorporated the MPS into their operations and whether there were any impediments to the operationalisation of the MPS;
  - c) any unintended consequences, or other issues, including on the effectiveness and efficiency of the agencies;
  - d) the comments and views of relevant oversight bodies, including the Inspector-General of Intelligence and Security (IGIS) and Government agencies.
5. In reviewing these MPSs we also considered the Report of the *Royal Commission of Inquiry into the terrorist attack on Christchurch masjidain on 15 March 2019* (Royal Commission Report) and the comments they made in relation to information collection.
6. We worked closely with the IGIS and his office, to ensure the revised MPSs provide the right level of assistance in supporting their oversight role.

## Some changes are common to all eleven MPSs

---

7. All MPSs have been amended to:
  - a) Include a cover sheet (or website landing page). The cover sheet sets out the overarching purpose of the MPSs, so each individual MPS just focuses on the specific activity it covers;
  - b) Improve readability, by simplifying the language (including the titles of the MPSs) and reducing repetition;
  - c) Separate the context (which is of more interest to the public) and the guidance to the agencies;
  - d) Clarify that the MPS only applies to lawful activity, and set out the legal obligations in relation to the activity covered by the MPS; and
  - e) Set out that the agencies are public service agencies and must comply with policies and procedures common to all New Zealand public service agencies.

### Changes have been made that are consistent across the information collection MPSs

8. For the three information collection MPSs, we have also included a description of the information collection framework – setting out the methods the agencies use to perform their statutory functions, and revising the scope sections to clearly specify what is in scope of each MPS, what is out of scope and what is within scope of another MPS. This is as the result of feedback that it could be confusing to know which MPS applied to which activity.
9. Descriptions of each MPS, the consultation undertaken during the review and the proposed revisions (in addition to those in the paragraphs above) are set out below.

## Collecting human intelligence MPS

---

10. The *Collecting Human Intelligence MPS* sets out your expectations, as responsible Minister, for how GCSB and NZSIS properly collects information from individuals (referred to as human intelligence) without an intelligence warrant or authorisation under the Act. In addition to the GCSB, NZSIS and the IGIS, New Zealand Police and the Privacy Commissioner were consulted:
11. The main changes to this MPS are:
  - The context section has been made clearer and has been simplified;
  - The 'warnings' section has been revised to provide more guidance to the agencies on how to make a statement to people they engage with that is intended to deter a person from a particular course of action. The MPS now stipulates that the agencies must have an internal policy to guide this activity;
  - A separate 'conflicts of interest' section has been added, to be clear that employees should not be involved in operations where a conflict of interest exists;

- It now specifies that foreign implications may also arise in relation to domestic human intelligence activity, not just in overseas intelligence activity, and in these circumstances the agencies must consult MFAT.

## Publicly available information MPS

---

12. The *Publicly Available Information MPS* sets out your expectations on how GCSB and NZSIS properly obtain, collect and use publicly available information. In addition to the GCSB, NZSIS and the IGIS, the following agencies were consulted:
  - Government Chief Privacy Officer;
  - Ministry of Justice;
  - New Zealand Police; and
  - The Privacy Commissioner.
13. The main feedback on this MPS was that it was focused on the use of publicly available information in relation to specific persons of interest. One of the findings of the Royal Commission Report was that collecting information for target discovery purposes was problematic under the current authorising environment. The Publicly Available Information MPS was an example of this.
14. The revised MPS has been re-framed to capture the broader range of uses of publicly available information, including for target discovery. The range of uses has been described. Other changes include:
  - The MPS now includes a requirement that the agencies have an internal policy that provides guidance on the collection, use, retention and disposal of large personal datasets that were obtained through collecting publicly available information;
  - It includes an example to demonstrate the applicability of section 19 of the Act (which provides that the exercise of the right to freedom of expression does not justify activity by an intelligence and security agency) in relation to publicly available information.
15. In addition, we received recommendations for operational detail (particularly to align with NZ Police's collection and use of publicly available information) that will be reflected in the NZSIS and GCSB's internal guidance.

## Section 121 requests MPS

---

16. The *Section 121 requests MPS* sets out your expectations for how the agencies make requests under section 121 of the Act. Section 121 of the Act recognises the existing ability of the GCSB and NZSIS to request information from other agencies, where the Director-General believes the information is necessary to enable the agency to perform their functions.
17. In addition to the GCSB, NZSIS and the IGIS, New Zealand Police and the Privacy Commissioner were consulted.

18. The main changes to this MPS are:

- It now clarifies the scope of a section 121 request. The previous MPS used the term 'formal requests', which was not clear to operational staff. The revised MPS includes more information about what is in and out of scope;
- It has been revised to make it clear that section 121 requests can include requests for information to assess the validity of leads;
- The oversight section now sets out that the way in which section 121 requests are recorded may depend on the request (including a saved email).

### **There are no outstanding issues from the consultation**

19. All agencies we consulted were given an opportunity to provide feedback on the second revised draft of the MPS. If any feedback was not taken on board, we provided justification for this, which the agencies have accepted. As far as we are aware, there are no remaining differences in views.
20. The IGIS has commented that the revised MPSs are a vast improvement on the existing versions.

### **Next steps**

21. If you agree with the proposed revisions, we recommend you sign the attached letters to send to your ministerial colleagues, as required under the Act. The 2017 versions of the MPSs are attached to send to your colleagues, along with the revised version of the MPS. We have not provided a tracked change version as the changes are too extensive for this to be useful. However the letters outline the main changes.
22. Once you receive any feedback from your consultation, we will amend the MPSs to reflect the comments, if you wish. The MPSs can then be finalised and reissued, along with the others that have already been reviewed.

<b>Attachments:</b>		
<b>Attachment A:</b>	UNCLASSIFIED	Draft revised Ministerial Policy Statement: Collecting Human Intelligence
<b>Attachment B:</b>	UNCLASSIFIED	2017 version of Ministerial Policy Statement: Collecting information lawfully from persons without an intelligence warrant or authorisation given under section 78 of the Intelligence and Security Act 2017
<b>Attachment C:</b>	UNCLASSIFIED	Draft revised Ministerial Policy Statement: Publicly Available Information
<b>Attachment D:</b>	UNCLASSIFIED	2017 version of Ministerial Policy Statement: Obtaining and Using Publicly Available Information
<b>Attachment E:</b>	UNCLASSIFIED	Draft revised Ministerial Policy Statement: Section 121

<b>Attachment F:</b>	UNCLASSIFIED	2017 version of Ministerial Policy Statement: Requesting Information from agencies under section 121 of the Intelligence and Security Act 2017
<b>Attachment G:</b>	UNCLASSIFIED	Letter to Hon Kris Faafoi, Minister of Justice
<b>Attachment H:</b>	UNCLASSIFIED	Letter to Hon Dr David Clark, Minister for Digital Economy and Communications
<b>Attachment I:</b>	UNCLASSIFIED	Letter to Hon Poto Williams, Minister of Police

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982



# ATTACHMENT A

## Draft revised Ministerial Policy Statement: Collecting Human Intelligence

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982



## *Ministerial Policy Statement*

# Collecting human intelligence

### Summary

The GCSB and NZSIS collect information from individuals on a regular basis for the performance of their functions. This collection activity, also referred to as human intelligence activity<sup>1</sup>, can be carried out on an ordinarily lawful basis without an intelligence warrant or authorisation under section 78 of the Act.

This Ministerial Policy Statement (MPS) provides guidance for the GCSB and NZSIS when collecting human intelligence without an intelligence warrant or specific authorisation under the Act. When collecting human intelligence, GCSB and NZSIS must have regard to the following principles: legal obligations, necessity, proportionality, minimal impact on third parties, appropriate conduct 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

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

### CONTEXT

#### Collecting human intelligence occurs within a wider information collection context

1. GCSB and NZSIS obtain or collect information through a range of methods authorised under the Act in order to perform their statutory functions. These authorities include:
  - a. Intelligence warrant;
  - b. Business records directions;

<sup>1</sup> The Act defines **human intelligence activities** as activities that involve the use of any person to gather intelligence.

- 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 [LINK]
    - iii. by collecting, requesting and receiving information from a person (known as human intelligence activities) (this MPS)
    - iv. from overseas public authorities (guidance on cooperation with overseas public authorities is addressed in [LINK])
  - b. Obtaining, collecting and using publicly available information [LINK]
  - c. Through the conduct of other lawful activities, such as conducting surveillance in a public place [LINK].

#### **Human intelligence activities**

3. Collecting intelligence is a statutory function of the GCSB and NZSIS. When a GCSB or NZSIS employee collects, requests or receives information directly from a person (rather than through the interception of communications or seizure of information) it is often referred to as human intelligence (or 'HUMINT').
4. Human intelligence can come from a range of sources – from covert human intelligence sources at one end of the spectrum, to private individuals who independently offer information, at the other end. There is also a broad range of human intelligence activities. For example, human intelligence activities include:
  - interviewing individuals that have knowledge, or access to knowledge, of interest;
  - building long-term relationships with someone with connections to a person or a group of security concern, or with access to information or foreign intelligence of value to the New Zealand Government; and
  - engaging openly with the public or community members.
5. Human intelligence can enhance intelligence obtained from other sources, help ascertain a person's intentions, identify matters or other people of security concern, and eliminate individuals or matters from investigations.
6. GCSB and NZSIS employees may carry out human intelligence activities on the following basis:
  - Declared (where the person is aware an employee is from the GCSB and NZSIS); or

- Undeclared (where the employee purports to be from the New Zealand Government but not from GCSB and NZSIS) or non-official (where the officer purports to be from outside of government). Collecting information from individuals on a clandestine or covert basis may allow GCSB and NZSIS to obtain information that a person would otherwise not disclose to them.
7. While the two agencies have consistent objectives and functions, each has distinct specialist capabilities. GCSB specialises in signals intelligence and information assurance and cybersecurity activities, while NZSIS specialises in human intelligence activities. Collecting human intelligence is an important tool used by the GCSB and NZSIS to help fulfill their statutory objectives. Other New Zealand government agencies with intelligence collection or law enforcement functions use the same methods for their own statutory purposes.
  8. Human intelligence collected by GCSB and NZSIS is rarely used as evidence in criminal proceedings. However, to the extent that it might be, the usual rules and protections will apply in every case, including those set out in the Evidence Act 2006.
  9. Mere exposure of the fact that human intelligence activities have been carried out by GCSB or NZSIS could pose reputational risk for the New Zealand Government. There is also a risk that, if something goes wrong with an operation, employees or the person providing the information could be put in danger. In addition, this could have a reputational or diplomatic risk to GCSB, NZSIS or the New Zealand Government more broadly, and may impact negatively on public trust and confidence in GCSB and NZSIS and public willingness to engage with the agencies. Because of the nature of these activities and the risks posed by them, specific guidance in the form of this MPS is appropriate.

## **GUIDANCE FOR GCSB and NZSIS**

---

### **Scope of this MPS**

10. This MPS applies to lawful human intelligence activities carried out by GCSB and NZSIS employees in the performance of their intelligence collection and analysis function. If the activity is otherwise unlawful, an authorisation under Part 4 of the Act is required before the activity may be carried out.
11. This MPS applies regardless of whether intelligence is collected from a person in a face-to-face meeting, over the internet, or via another form of communication.
12. When carrying out human intelligence activities, GCSB and NZSIS employees may use a range of tools and methods for obtaining information that are subject to separate ministerial guidance. When this occurs, the activity must be conducted in accordance with the guidance in this MPS as well as other relevant ministerial guidance. For example, when employees:
  - carry out human intelligence activities using an assumed identity, this MPS should be read alongside the MPS on *Assumed identities* [LINK];
  - make a false and misleading representation about their employment during the course of human intelligence activities, this MPS should be read alongside the MPS on *False or misleading representations about employment* [LINK];

- request information to be voluntarily disclosed by another agency under section 121 of the Act, this MPS should be read alongside the MPS on *Section 121 Requests* [LINK].

13. This MPS does not apply to:

- activities carried out as part of routine administrative and business functions, which are common to most public service departments. For example, activities carried out as part of procurement or employment processes;
- collection of information that is publicly available as set out in the MPS: *Publicly available information* [LINK];
- activities carried out for the purposes of providing protective security services, advice and assistance. For example, activities carried out by the GCSB for the purposes of providing consented information assurance and cybersecurity. Such activity is covered by a separate MPS, *Providing information assurance and cybersecurity activities* [LINK];
- requests for information made by GCSB to facilitate its regulatory function under Part 3 of the Telecommunications (Interception Capability and Security) Act 2013;

### **Principles**

14. The following principles constitute a framework for good decision making and set out best practice conduct. They must be taken into account by GCSB and NZSIS employees when planning and conducting human intelligence activities. All human intelligence activities, particularly those conducted on a long term basis, should be subject to ongoing review as to whether they continue to be consistent with these principles.

### **Legal obligations**

15. Where human intelligence activities involve the collection of personal information, the Privacy Act 2020 will apply, including information privacy principle 4(a) which states that personal information shall not be collected by unlawful means.
16. GCSB and NZSIS may remunerate human sources but must not engage in any activity that could be understood as coercion, blackmail, entrapment, or harassment.
17. Employees must avoid tasking, encouraging, or condoning any unlawful activity in New Zealand. Employees must not imply or suggest that they have the power or authority to offer favourable treatment in official or judicial processes, such as immigration or citizenship determinations, or in criminal or civil proceedings. Criminal immunity is only available in respect of activities conducted pursuant to an authorisation, or in circumstances envisaged by section 111 of the Act.
18. Where appropriate, legal advice should be sought during the planning and conduct of human intelligence activities.

### **Necessity**

19. Human intelligence activities can be carried out when necessary to enable GCSB and NZSIS to perform their statutory functions. This includes activities for the purposes of security, training, or

the development of capabilities. For the avoidance of doubt, this also includes carrying out human intelligence activities to assess the validity of lines of enquiry or leads. GCSB and NZSIS may also need to collect similar or the same information from a range of different people, including for the purposes of assessing the reliability of the information.

20. The principle of necessity reflects the law in relation to the collection of personal information. Information privacy principle 1 in 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.

### ***Proportionality***

21. The impact of human intelligence activities should be proportionate to the purpose, including the anticipated outcomes of the activity.
22. When assessing the proportionality of human intelligence activities, the GCSB and NZSIS must consider the scope of the proposed activity, the risk the activity poses to the person providing the information, employees, and third parties, and reputational risks to GCSB, NZSIS and the New Zealand Government more broadly if the activity is compromised. The level of intrusion into the affairs of a person is also relevant to a proportionality assessment. Consideration should always be given to whether the information sought has already been collected and, if not, whether it can be collected in a different and less intrusive way.
23. GCSB and NZSIS should also have regard to possible risks to the individual within the community from which the person providing information comes, and between the community and the state, particularly in the case of a minority community.

### ***Minimal impact on third parties***

24. The possible impact of human intelligence activities on persons who are not relevant to the matter about which information is sought should be considered. Any impact on third parties should be limited as far as practicable, and any adverse impacts should be considered in light of the necessity principle and be proportionate to the purpose of the activity.

### ***Oversight***

25. GCSB and NZSIS must carry out all activities in a manner that facilitates effective oversight, including through the keeping of appropriate records about the planning, approval, conduct, and reporting of human intelligence activities.

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

26. As public service agencies, GCSB and NZSIS must comply with legislation, policies and procedures common to all New Zealand public service agencies.<sup>2</sup>
27. In addition, where relevant to their activities GCSB and NZSIS must have, and comply with, internal policies and procedures that are consistent with the requirements and principles of this MPS, and

---

<sup>2</sup> This includes the Public Service Act 2020 and the Health and Safety at Work Act 2015.

must have systems in place to support and monitor compliance. These policies and procedures must also address the following matters:

- ***Procedural fairness***

GCSB and NZSIS employees must make reasonable efforts to ensure interviewees understand that an interview is an opportunity to provide comment to inform any assessment NZSIS and / or GCSB may make.

GCSB and NZSIS must apply general standards of procedural fairness. What is required will depend on the particular circumstances, and the types of measures required to ensure procedural fairness will be set out in internal guidance. For example, where relevant, the purpose of an interaction or interview with a member of the public should be made clear, as well as the voluntary nature of the interview and lack of any enforcement powers available to the agencies. This information, and other relevant information regarding the agencies' roles and functions and individuals' rights when being questioned by the agencies, should be made available to the public via the agencies website

- ***Representations***

To perform their statutory functions it will sometimes be necessary for GCSB and NZSIS employees to make certain representations to people to protect sensitive information or to prevent operational activity being revealed (see MPSs on *False or misleading representations about employment* [LINK] and *Assumed identities* [LINK]). Such representations are a legitimate intelligence tool. But there are some types of representations that are not appropriate in the course of human intelligence activities.

GCSB and NZSIS employees may not represent to individuals they interact with that the GCSB and NZSIS have enforcement powers or the ability to compel the provision of information or assistance without authorisation under the Act. Similarly, when carrying out otherwise lawful human intelligence activities, employees must not represent themselves as having the power to compel the provision of information, to require assistance, to detain a person, to demand entry to private premises, or to offer immunity from criminal liability.

- ***Warnings***

It may be acceptable, in some cases, for declared employees to make a statement to persons they engage with that is designed, intended, or would reasonably be understood to be intended, to deter a person from a specific course of conduct. For example, an employee may warn that plans to travel to participate in politically motivated violence may be dangerous, illegal, and may result in the government taking action to prevent travel. Employees must take care to ensure that a warning does not constitute enforcement action, which is not a function of GCSB and NZSIS (section 16 of the Act).

Where such action is contemplated, GCSB and NZSIS employees should consider whether the warning would be more appropriately delivered by the Police or another agency with enforcement functions.

Internal policies should require legal advice and any other advice to be sought where appropriate.

- **Remuneration**

GCSB and NZSIS must have a policy in place to provide guidance on remunerating individuals that are human sources.

- **Conflicts of interest**

Employees should not be involved in operations where a conflict of interest exists, including any conflict of interest arising by reason of a familial or very close personal relationship.

GCSB and NZSIS should also ensure their employees are aware of the limits of their influence in respect of the people they engage with, including limits to personal relationships.

- **Sensitive category individuals**

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, refugees and asylum seekers, New Zealand Members of Parliament, members of the New Zealand Judiciary and journalists).

Some categories of sensitive persons are capable of making independent decisions in their own best interests, while other categories will be less capable of doing this. For this reason, children and young people, and people with diminished mental capacity will not be actively sought as sources. If another form of engagement with them is considered necessary, appropriate safeguards (such as the involvement of a guardian) will be applied.

Authorisation at a senior level within the relevant agency is required for activities conducted in respect of sensitive category individuals. This will ensure that appropriate measures are in place if human intelligence activities need to be carried out in respect of these individuals.

- **Information protected by privilege**

GCSB and NZSIS must have a policy setting out the restrictions and protections necessary when carrying out activities that may involve the collection of statutorily prescribed classes of privileged information. For example, information attracting legal or medical privilege or privileged information with regard to ministers of religion.

- **Health and safety**

All human intelligence activities must be undertaken consistently with GCSB's and NZSIS's obligations under the Health and Safety at Work Act 2015. In addition, GCSB and NZSIS may owe a duty of care to persons recruited as a source in the context of human intelligence activities. GCSB and NZSIS must carefully assess any risks to the welfare of that source and take all reasonable steps to mitigate them.



- **Training**

All GCSB and NZSIS employees involved in the conduct of human intelligence activities should be appropriately trained for the role they are expected to undertake and should be aware of all relevant laws, policies and procedures. Training needs should be considered and undertaken regularly to ensure all employees' training remains up to date.

- **Human intelligence activities with foreign relations implications**

The conduct of lawful human intelligence activities overseas could have significant foreign relations implications if compromised. Similarly, the risk to staff conducting human intelligence activities overseas is likely to be greater than operations conducted domestically.

If human intelligence activity, whether conducted in New Zealand or overseas, is predicted to involve significant risk to New Zealand's foreign policy or international relations, GCSB and NZSIS must consult with the Ministry of Foreign Affairs and Trade (MFAT). Where lawful human intelligence activities are to be conducted overseas, regard must be had to any existing guidance, protocol, or agreement between NZSIS/GCSB and MFAT in respect of such activities and the MPS on *Cooperating with overseas public authorities* [LINK].

- **Cooperation with and assistance from other agencies**

Where human intelligence activities are carried out with assistance from other agencies, GCSB and NZSIS remain responsible for the conduct of these activities and the actions of employees of other agencies. All such activities will be open to inquiry by the Inspector-General of Intelligence and Security. Any employees of other agencies who assist GCSB and NZSIS in the conduct of human intelligence activities should be appropriately trained for the role they are expected to undertake and should be aware of all relevant GCSB and NZSIS policies and procedures.

Where human intelligence activities are carried out alongside or in cooperation with another agency's operations, each agency shall remain subject to their own internal controls and subject to their usual oversight mechanisms.

Where human intelligence activities are carried out with the assistance of foreign agencies, the MPS on *Cooperating with overseas public authorities* will also apply.

- **Information management**

Information collected through human intelligence activities 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 MPS on *Information management* applies in relation to management of this information.

- **Compliance with the information privacy principles**

GCSB and NZSIS are subject to information privacy principles 1, 4(a), and 5 to 13 in the Privacy Act 2020. Policies relating to human intelligence activities and the handling of any

information collected through such activities must incorporate guidance about compliance with the relevant information privacy principles.

#### **Authorisation procedures**

28. Human intelligence activities should be authorised at a level of seniority within GCSB and NZSIS that is commensurate with the level of operational, reputational, and legal risk involved. The level of authorisation required should be determined by the nature of the activity and the assessed overall residual risk exposure. For example, as set out above, authorisation at a high level will be required for activities conducted in respect of sensitive category individuals.
29. The identification and management of operational, reputational, legal, and health and safety risks should be carried out in accordance with a risk management policy.
30. The Directors-General of the GCSB and NZSIS should have delegations in place for such authorisations.

#### **Duration of Ministerial Policy Statement**

31. This MPS will take effect from XX November 2021 for a period of three years. The Minister who issued a MPS may, at any time, amend, revoke or replace the MPS.

## ATTACHMENT B

2017 version of Ministerial Policy Statement: Collecting information lawfully from persons without an intelligence warrant or authorisation given under section 78 of the Intelligence and Security Act 2017

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982



## *Ministerial Policy Statement*

# Collecting information lawfully from persons without an intelligence warrant or authorisation given under section 78 of the Intelligence and Security Act 2017

### **Summary**

The Government Communications Security Bureau (GCSB) and the New Zealand Security Intelligence Service (NZSIS) collect information lawfully from persons without an intelligence warrant or authorisation given under section 78 on a regular basis. Those lawful activities can be broadly described as human intelligence activities. Those activities may involve an element of covertness or misrepresentation, but this is not always the case. This ministerial policy statement (MPS) provides guidance about the conduct of human intelligence activities. In doing so, GCSB and NZSIS must have regard to the following principles: legality, necessity, proportionality, less intrusive means to be considered, minimal impact on third parties 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.

*GCSB* means the Government Communications Security Bureau.

*NZSIS* means the New Zealand Security Intelligence Service.

### **Purpose**

1. This MPS is issued by the Minister Responsible for the GCSB and the NZSIS pursuant to section 206(d) of the Intelligence and Security Act 2017.
2. The purpose of this MPS is to provide guidance to GCSB and NZSIS on the collection of information lawfully from persons without an authorisation (commonly referred to as 'human intelligence activities'). The MPS comprises the Minister's expectations for how GCSB and NZSIS should

properly perform their functions and establishes a framework for good decision-making and best practice conduct.

3. MPSs are also relevant to oversight of the agencies by the Inspector-General of Intelligence and Security in the exercise of their propriety jurisdiction (the Act requires the Inspector-General of Intelligence and Security to take account of any relevant MPS and the extent to which an agency has had regard to it when conducting any inquiry or review).
4. Every employee making decisions or taking any action relating to collecting information lawfully from persons within the scope of this MPS must have regard to this MPS. Employees should be able to explain how they had regard to the MPS. This might amount to an explanation of their consideration of any relevant internal policy or procedures that reflect the MPS. The Directors-General are responsible for ensuring the MPS is reflected in their agency's internal policies and procedures. If any action or decision is taken that is inconsistent with the MPS, employees must be able to explain why the action was taken and how they had regard to the MPS.

### Scope

5. This MPS applies to the collection of information lawfully from persons without an intelligence warrant or authorisation given under section 78 of the Act. It is intended to cover lawful human intelligence activities (or 'HUMINT'). Human intelligence is obtained from people with knowledge of or access to information. Human intelligence may come from a range of sources – from covert human intelligence sources at one end of the spectrum, to private individuals who independently offer information, at the other end. This means human intelligence activities include a broad array of activities, from working with covert human sources and protecting them by helping them conceal their involvement with GCSB and NZSIS, through to engaging openly with community members or interested members of the public.
6. This MPS applies regardless of whether information is collected from a person in a face-to-face meeting, over the Internet, or via any other form of communication. Where information is collected through the use of an assumed identity this MPS should be read in conjunction with the MPS on *Acquiring, using, and maintaining an assumed identity*.
7. The agencies regularly request information from other organisations and individuals in the performance of their functions (for example, they may approach a business to confirm address details through billing records). These requests are always made overtly; that is, it is clear that the requester is from an intelligence and security agency. This MPS does not cover those types of information gathering activities, which are covered by a separate MPS (see MPS on *Requesting information from agencies under section 121*).
8. Nor does this MPS cover the creation, maintenance, and use of assumed identities or corporate identities for the purpose of undertaking intelligence collection or other activities, false and misleading representations relating to employment with an intelligence and security agency (that is, personal cover), or open source intelligence collection. Those activities are covered by separate MPSs (see *Making false or misleading representations under section 228 about being employed with an intelligence and security agency* and *Obtaining and using publicly available information*).
9. This MPS only relates to ordinarily lawful human intelligence activities; it does not therefore cover unlawful human intelligence activities that may only be carried out under an authorisation. Such activities must be conducted in accordance with the terms of that authorisation, including any restrictions or conditions set out in the authorisation.

## Context

10. GCSB's and NZSIS's objectives are set out in the Act. Both agencies contribute to:
  - a) The protection of New Zealand's national security;
  - b) The international relations and well-being of New Zealand; and
  - c) The economic well-being of New Zealand.
11. GCSB and NZSIS do this through the performance of their statutory functions, which include:
  - d) Intelligence collection and analysis; and
  - e) The provision of protective security services, advice and assistance.
12. While the two agencies have consistent objectives and functions, each has distinct specialist capabilities. GCSB specialises in signals intelligence and information assurance and cybersecurity activities, while NZSIS specialises in human intelligence activities.
13. MPSs are an important component of the measures put in place by the Act to ensure the functions of GCSB and NZSIS are performed with propriety and in accordance with New Zealand law and all human rights obligations recognised by New Zealand law.
14. To perform any of their statutory functions, it is necessary for GCSB and NZSIS to use a range of methods to collect information. This includes collecting information from people in an entirely open manner (for example, by a declared member of GCSB or NZSIS asking for and receiving information), or on a clandestine and/or covert basis (for example, a member of GCSB or NZSIS making the same request without declaring that they work for GCSB or NZSIS, which may include the use of an assumed identity). Collecting information from persons on a clandestine and/or covert basis may allow GCSB or NZSIS to obtain information that a person would otherwise not disclose to them.
15. In some cases, members of GCSB and NZSIS may build up long-term relationships with people and collect information from them over the course of that relationship. Collecting information from people is an important and legitimate element in the toolkit of GCSB and NZSIS. Other New Zealand government agencies with intelligence collection and law enforcement functions also use the same methods for their own statutory purposes.
16. By way of example, human intelligence activities may involve developing a relationship with a person with connections to a person or group of security concern in order to obtain an insight into what the latter are saying and planning. That information may be helpful in ascertaining their intentions, identifying other people of security concern, and eliminating individuals from investigations. At the other end of the spectrum it may involve a one-off, voluntary disclosure of information from a concerned member of the public.
17. Mere exposure of the fact that human intelligence activities have been carried out by GCSB or NZSIS would pose reputational risk for the New Zealand Government. There is also a risk that, if something goes wrong with an operation, employees and/or the person providing the information could be put in danger. In addition, this could have a reputational or diplomatic risk to GCSB, NZSIS, or the New Zealand Government more broadly, and may impact negatively on public trust and confidence in the agencies and public willingness to engage with the agencies. Because of the nature of these activities and the risks posed by them, specific guidance in the form of this MPS is appropriate.

## Principles

18. The following principles constitute a framework for good decision-making and must be taken into account by GCSB and NZSIS when they are planning and conducting human intelligence activities. All human intelligence activities, particularly those conducted on a longer term basis, should be subject to ongoing review as to whether they continue to be consistent with these principles.

### *Legality*

19. Human intelligence activities must be carried out in accordance with the law. Where appropriate, legal advice should be sought during the planning and conduct of human intelligence activities. If the activity is otherwise unlawful or if its lawfulness could reasonably be considered unclear, an authorisation under Part 4 of the Act will be required before the activity may be carried out.
20. Where human intelligence activities involve the collection of personal information, [information privacy principle 4](#) of the Privacy Act 1993 will apply. That information privacy principle requires that personal information be collected by lawful means.
21. The use of an assumed identity by an employee of GCSB or NZSIS in carrying out human intelligence activities would require authorisation by the Directors-General under Part 3 of the Act for the use of that assumed identity.
22. GCSB and NZSIS may remunerate human sources but must avoid any form of approach or cultivation that could be understood as coercion, blackmail, entrapment, bribery or harassment.
23. Employees must avoid tasking, encouraging, or condoning any unlawful activity, or other behavior (online or otherwise) that is of security concern. Similarly, agency employees must not imply or suggest that they have the power or authority to offer favourable treatment in official or judicial processes, such as immigration or citizenship determinations, or in criminal or civil proceedings. Criminal immunity is only available in respect of activities conducted pursuant to an authorisation and in circumstances envisaged by section 111 of the Act; it will not be relevant in respect of activities undertaken in respect of this MPS, which applies only to *lawful* human intelligence activities.
24. It may be acceptable for employees collecting human intelligence to give people they engage with advice – including, as appropriate, advice about possible negative repercussions of certain conduct. This may include warning an individual about the wisdom of certain activities; for example, an employee may warn that plans to travel to participate in violent jihad may be dangerous, illegal and may result in the government taking action to prevent the travel. However, this sort of action may – depending on the circumstances – constitute enforcement action, which is not a function of the agencies (subject to the terms of section 16). In such circumstances, it may be necessary to consider whether advice that amounts to a warning would be more appropriately delivered by the Police or another agency with enforcement functions. In any circumstances where such action is contemplated, the agencies' internal policies should require legal advice to be sought (including from Crown Law office, where appropriate).

### *Necessity*

25. Human intelligence activities should only be carried out when necessary to enable GCSB or NZSIS to perform their statutory functions. Those activities – including those needed for security, training, or the development of capabilities – should be directed towards the performance of those functions. In some circumstances, it may be necessary for GCSB or NZSIS to collect similar or the same information from a range of different persons – for example, where GCSB or NZSIS

need to obtain the information from a number of sources in order to assess the reliability of the information.

26. This reflects the law in relation to the collection of personal information – [information privacy principle 1](#) of the Privacy Act 1993 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.

#### *Proportionality*

27. The impact of human intelligence activities should be proportionate to the purpose, including the anticipated benefits.
28. When assessing the proportionality of human intelligence activities, the agencies must consider the scope of the proposed activity, the level of intrusion into the affairs of a person, the risk the activity poses to the person providing the information, employees, and third parties, and the reputational risks to GCSB/NZSIS and the New Zealand Government more broadly if the activity is compromised in some way. The agencies should also have regard to possible risks to the relationship between the community from which the person providing information comes and the state, particularly in the case of a minority community.

#### *Less intrusive means to be considered*

29. Consideration should always be given to whether the information sought has already been collected and, if not, whether it can be collected in a different and less intrusive way. Carrying out lawful human intelligence activities may also be a less intrusive method of meeting an intelligence need than carrying out an otherwise unlawful activity with an authorisation under Part 4 of the Act.

#### *Minimal impact on third parties*

30. The possible impact of human intelligence activities on persons who are not relevant to the matter about which information is sought should be considered. Any impact on third parties should be limited as far as practicable, and any adverse impacts should be considered in light of the necessity principle and proportionate to the purpose of the activity.

#### *Oversight*

31. GCSB and NZSIS must carry out all activities in a manner that facilitates effective oversight, including through the keeping of appropriate records about the planning, approval, conduct, and reporting of human intelligence activities.



## Matters to be reflected in internal policies and procedures

32. GCSB and NZSIS must have, and act in compliance with, internal policies and procedures that are consistent with the requirements and principles above, and must have systems in place to support and monitor compliance. These policies and procedures must also address the following matters:

### **Appropriate conduct, including compliance with public service minimum standards of integrity and conduct**

The Directors-General of GCSB and NZSIS must issue policies and procedures that reflect the agencies' obligations under the Public Service Act 2020.

GCSB and NZSIS must have internal policies that address its employees' obligations in respect of the collection of information from, or relating to, people they know in a personal capacity. Employees should not be involved in operations where a conflict of interest exists, including any conflict of interest arising by reason of a familial or very close personal relationship.

Both agencies should also ensure their employees are aware of the limits of their influence in respect of people they engage with, including limits to personal relationships.

### **Procedural fairness**

GCSB or NZSIS employees must make reasonable efforts to ensure interviewees understand that an interview is an opportunity to provide comment to inform any assessment GCSB/NZSIS may make. Employees must ensure the individual is clear that GCSB/NZSIS has no enforcement powers and that their actions cannot be interpreted as coercive or as applying undue pressure.

The agencies' policies must also make it clear that general standards of procedural fairness apply. What is required in any particular situation will depend on the circumstances. The agencies' policies must provide guidance on the types of measures that might be required to ensure procedural fairness and when these will apply. When interacting with members of the public, where relevant, the purpose of the interaction or interview should be made clear, as well as the voluntary nature of the interview and lack of any enforcement powers available to the agencies. This information, and any other relevant information regarding the agencies' roles and functions and individuals' rights when being questioned by the agencies, should be made available to the public via the agencies' websites.

### **Sensitive category individuals**

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, Members of New Zealand's Parliament, members of the New Zealand judiciary, journalists, lawyers, registered medical practitioners or other providers of health services attracting medical privilege, and people vulnerable by reason of illness or other incapacity).

Some of these categories of sensitive persons are fully capable of making independent decisions in their own best interests, while other categories will be less capable of doing this. For this reason children and young people and people with diminished mental capacity will not be actively sought as sources and if engagement with them is considered necessary, appropriate safeguards (such as the involvement of a guardian) will be applied.

Authorisation at a high level within the relevant agency is required for activities conducted in respect of these individuals. This will provide reassurance that appropriate measures are in place in the event human intelligence activities need to be carried out in respect of sensitive category individuals.

### **Health and safety**

All human intelligence activities must be undertaken consistently with GCSB's and NZSIS's obligations under the Health and Safety at Work Act 2015. In addition, GCSB and NZSIS will often owe a duty of care to any person recruited as a source in the context of human intelligence activities. The agencies must carefully assess risks to the welfare of that source and take all reasonable steps to mitigate them.

### **Training**

All GCSB and NZSIS employees involved in the conduct of human intelligence activities should be appropriately trained for the role they are expected to play and should be aware of all relevant laws, policies, procedures, and other obligations such as those arising from the Health and Safety at Work Act 2015. Training needs should be considered and addressed regularly to ensure all employees' training remains up to date.

### **Use of information collected from human intelligence activities**

Information collected by GCSB and NZSIS by means of lawful human intelligence activities is collected for intelligence purposes. Such information is rarely used as evidence in criminal proceedings. However, to the extent that it might be, the usual rules and protections will apply in every case, including those set out in the Evidence Act 2006.

### **Human intelligence activities undertaken overseas**

The conduct of lawful human intelligence activities overseas could have significant foreign relations implications if security is compromised. Similarly, the risk to staff conducting human intelligence activities overseas is likely to be greater than operations conducted domestically.

If the activity is predicted to involve significant risk to New Zealand's reputation, GCSB and NZSIS must consult with the Ministry of Foreign Affairs and Trade (MFAT). Where lawful human intelligence activities are to be conducted overseas, regard must be had to any existing guidance, protocol, or agreement between GCSB/NZSIS and MFAT in respect of such activities and the MPS on *Cooperation with overseas public authorities*.

### **Cooperation with and assistance from other agencies**

Where human intelligence activities are carried out with assistance from other agencies, GCSB and NZSIS remain responsible for the conduct of these activities and the actions of employees of other agencies. All such activities will be open to inquiry by the Inspector-General of Intelligence and Security. Any employees of other agencies who assist GCSB and NZSIS in the conduct of human intelligence activities should be appropriately trained for the role they are expected to play and should be aware of all relevant policies and procedures.

Where human intelligence activities are carried out alongside or in cooperation with another agency's operations, each agency shall remain subject to their own internal controls and subject to their usual oversight mechanisms.

Where human intelligence activities are carried out with the assistance of foreign agencies, the MPS on Cooperation with overseas public authorities will also apply.

### **Representations**

To perform their statutory functions it will sometimes be necessary for GCSB or NZSIS employees to make certain representations to people to protect sensitive information, including identities of GCSB or NZSIS staff (see MPSs on *False or misleading representations about employment* and *Acquiring, using and maintaining an assumed identity*), or to prevent operational activity being revealed. For example, an officer might make a false statement about their identity or their reason for meeting. Such representations are a legitimate intelligence tool.

There are some types of representations that are not appropriate in the course of human intelligence activities. GCSB and NZSIS do not have enforcement powers or the ability to compel the provision of information or assistance without a warrant or authorisation. Employees may not represent to individuals they interact with that the agencies have enforcement powers. Similarly, employees must not represent themselves as having the power to compel the provision of information, to require assistance, to detain a person, to demand entry to private premises, or to offer immunity from criminal liability. It is expected GCSB and NZSIS will have clear policies to reinforce that employees must not make such representations.

### **Information management**

Information collected through the use of human intelligence may be among some of the more sensitive information held by GCSB and NZSIS, given it may include sensitive information about identifiable individuals. This information must be handled and stored with clear access controls that correspond to the sensitivity of the information. The MPS on *Management of information obtained by GCSB and NZSIS* will also apply in relation to management of this information.

### **Compliance with the information privacy principles**

GCSB and NZSIS are subject to [information privacy principles](#) 1, 4(a), and 5 to 12 of the information privacy principles in the Privacy Act 1993. All policies relating to human intelligence activities and the handling of any information collected through such activities must incorporate guidance about compliance with the information privacy principles.

## **Authorisation procedures**

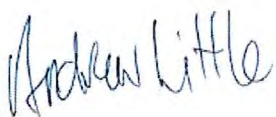
33. Human intelligence activities should be authorised at a level of seniority within GCSB and NZSIS that is commensurate with the level of operational, reputational and legal risk involved. The level of authorisation required should be dictated by the nature of the activity and the assessed overall residual risk exposure. For example, as set out above, authorisation at a high level will be required for activities conducted in respect of sensitive category individuals. The identification and management of operational, reputational, legal, and health and safety risks should be carried out in accordance with a risk management policy.
34. The Directors-General of each agency should have delegations in place for such authorisations.

### Duration of ministerial policy statement

35. This MPS will take effect from 28 September 2020 for a period of three years. The Minister who issued a 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

September 2020

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

# ATTACHMENT C

Draft revised Ministerial Policy Statement: Publicly Available Information

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982



## *Ministerial Policy Statement*

# Publicly available information

### Summary

It is lawful for GCSB and NZSIS to obtain, collect and use publicly available information. This ministerial policy statement (MPS) provides guidance on the conduct of this activity. In making decisions related to obtaining, collecting and using publicly available information, GCSB and NZSIS must have regard to the following principles: respect for privacy, necessity, proportionality, least intrusive means, respect for freedom of expression, including the right to advocate, protest or dissent, legality and oversight. This MPS also specifies certain matters to be included in internal policies and procedures.

### Definitions

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

**Open source intelligence** means intelligence products produced from publicly available information

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

**Publicly available information** means information that:

- a) is published in printed or electronic form or broadcast:
- b) is generally available to members of the public free of charge or on payment of a fee

**GCSB** means the Government Communications Security Bureau

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

### CONTEXT

**Obtaining, collecting and using publicly available information occurs within a wider information collection context**

1. GCSB and NZSIS obtain or collect information through a range of methods 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 [LINK];
    - 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 in [LINK])
    - iv. from overseas public authorities (guidance on cooperation with overseas public authorities is addressed in [LINK])
  - b. Obtaining, collecting and using publicly available information (this MPS).
  - c. Through the conduct of other lawful activities, such as conducting surveillance in a public place [LINK].

**Publicly available information**

3. To perform their functions, GCSB and NZSIS may access publicly available information. For example, the GCSB and NZSIS may need to access and obtain or collect information about an individual's social media posts, or their contacts or group memberships. GCSB and NZSIS may also collect publicly available information (including large data sets) in order to identify people, events, or activities of interest – for example, accessing or monitoring specific open online communities or social media platforms, or for reference purposes to support their functions more generally.
4. Publicly available information supports GCSB and NZSIS functions, including by developing different forms of open source intelligence. Publicly available information may be combined with other sources of information (including that obtained or collected under authorisations) to inform assessments and/or identify details that are not immediately obvious from a piece of information considered in isolation. Open source intelligence supports intelligence activity across all GCSB and NZSIS activity, including in operations, investigations, and maintaining situational awareness (for example, of the geo-political context). The range of uses include:
- a. discovering previously unidentified actors, events, or activities that may pose a risk to New Zealand's national security;
  - b. providing further information on identified individuals and threat actors (for example violent extremists);
  - c. supporting other sources to corroborate, support, or provide a counter-narrative;

- d. using indicators of compromise in providing consented cyber-security activities; and
- e. supporting vetting of security clearances.

## **GUIDANCE FOR NZSIS AND GCSB**

---

### **Scope of this MPS**

- 5. This MPS applies to the lawful collection and use by GCSB and NZSIS of information that is publicly available, including publicly available personal information.
- 6. People sharing information in a way that makes it able to be obtained by a member of the public would not necessarily have a reasonable expectation of privacy with regard to the use of that information (for example, in an open social media group, or Tweet). Publicly available information includes information shared within groups where there is an ability to 'opt in' with minimal restrictions or vetting of the membership of the group (for example simply providing an email or other login details). This level of scrutiny is usually about determining interest in the group, rather than verifying the real identities of those seeking access.
- 7. Online communities also exist where only people that are proactively approved members can view and/or participate. Such information could not be viewed by a member of the public without undergoing greater level of scrutiny than simply 'opting in' as outlined in [paragraph 6]. It would therefore be more likely for people sharing information this way to have a reasonable expectation of privacy. Information shared in this way is beyond the scope of this MPS, it may still be within the scope of an authorisation or activities outlined in the *Human Intelligence MPS* [LINK].
- 8. Information that is behind a paywall may still be publicly available information. For example, online forums or comment sections of publications that require a one-off payment or subscription are publicly available, or publicly available information that has been aggregated by a third party. GCSB and NZSIS must consider whether collecting publicly available information may be in breach of a service's terms and conditions and seek legal advice as appropriate on whether collecting information through this method requires additional authorisation. In providing information for creation of an account for a paywalled subscription, the MPS on Assumed Identities [LINK] or Legal Entities [LINK] must be considered as appropriate.

### **Principles**

- 9. The following principles constitute a framework for good decision-making and set out best practice conduct. They must be taken into account by GCSB and NZSIS when obtaining, collecting and using publicly available information. This activity should be subject to ongoing review as to whether it continues to be consistent with these principles.

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

- 10. There may be some privacy interests in publicly available information, particularly where that information is personal information. This does not preclude the agencies from collecting or using that information. As outlined in the *Information Management MPS* [LINK] protections applied to information may be able to mitigate privacy impacts. Such protections may include limiting the number of employees who may have access to analysis of personal information, or anonymising



personal information.

11. The right to privacy (in the form of freedom from unreasonable search and seizure) is protected by section 21 of the New Zealand Bill of Rights Act 1990. In addition, GCSB and NZSIS are subject to the Privacy Act 2020 and information privacy principles 1, 4(a), and 5-13 apply where the agencies have access to personal information.
12. Collecting publicly available personal information will activate the obligation under privacy principle 8 (an organisation must check that the information is accurate, up to date, complete and relevant before using). GCSB and NZSIS must take reasonable steps to check the accuracy of the information, including potentially collecting further publicly available information. This is relevant, for example, in performing the NZSIS's security vetting function.

### ***Necessity***

13. Publicly available information, including personal information, should only be obtained, collected and used for a purpose that is consistent with GCSB and NZSIS performing their statutory functions. GCSB and NZSIS should be clear that any activities involving the collection of publicly available information have a clear purpose, and ensure a purpose continues throughout the course of the collection and use of publicly available information.
14. Examples of purposes where it will be necessary to obtain, collect and use publicly available information include acquiring background or contextual information relevant to the performance of a statutory function, acquiring information to identify behavioural patterns of interest, collecting information for reference purposes and collecting information to assess the accuracy of information already held.
15. For reasons of operational security, GCSB and NZSIS may need to obfuscate their interest in certain information. This may be achieved by transferring a copy of a broader set of publicly available information to a secure environment before analysing the relevant information.

### ***Proportionality***

16. The collection and use of publicly available information should be proportionate to the purpose for which it is carried out. The amount of information may be one factor to consider when assessing proportionality. The age of the information may also be a consideration, as there may be an increased risk that the information is out of date and less likely to be fit for purpose.
17. Publicly available information may be collected and used to identify associates or contacts of a person of security concern. Publicly available information and analysis carried out using that information may contain personal information about individuals not relevant to the purpose for which information is sought. Where practicable, GCSB and NZSIS should minimise the collection of publicly available personal information about persons who are not relevant to the purpose for which information is sought.
18. Privacy principles 10 and 11 place limits on government agencies using and disclosing personal information. Certain exceptions (privacy principles 10(2) and 11(1(g))) allow for the GCSB or NZSIS

to use or disclose such information when there are reasonable grounds to believe the use or disclosure is necessary to enable GCSB or NZSIS to perform any of their functions.

***Least intrusive means***

19. In collecting publicly available information, GCSB and NZSIS must use the least intrusive means available to obtain or collect the required information in a secure, timely and reliable manner (noting that the collection of publicly available information is one of the least intrusive means of collection of intelligence).

***Respect for freedom of expression, including the right to advocate, protest, or dissent***

20. Section 19 of the Act provides that the exercise by any person in New Zealand or any class of persons in New Zealand of their right to freedom of expression under the law (including the right to advocate, protest, or dissent) does not itself justify an intelligence and security agency taking any action in respect of that person or class of persons.

21. GCSB and NZSIS must ensure collection of publicly available information related to advocacy, protest, or dissent is undertaken only where the purpose of doing so is necessary to enable the agency to perform one of its statutory functions. For example:

- a. Protesting, or planning a protest, will not be sufficient justification by itself for collecting information. If, however, a security concern arises, the agencies may be justified in collecting publicly available information about the threats. One indication of a security concern could be if the views expressed in the protest include a serious threat to lives or security.
- b. Public expression of certain views will generally not be sufficient justification on its own for collecting publicly available information. However, if there are security concerns about the views that are expressed (such as advocating online a serious threat to lives or security), this might provide justification for collecting information.

***Legal obligations***

22. GCSB and NZSIS must ensure that the collection and use of publicly available information will be carried out in accordance with the law. Care must be taken to ensure that only publicly available information is collected – unless the agencies have a warrant or other authorisation under the Act. Where appropriate, or if there is any doubt, legal advice should be sought.

23. GCSB and NZSIS may collect publicly available information using collection methods that are not available to the public (for example, by using specialist techniques for collecting information). The agencies must take particular care to ensure that any collection of publicly available information using methods not available to the public does not involve any unlawful activity, unless done so with an authorisation under Part 4 of the Act.

24. GCSB and NZSIS must have regard to the statutes that establish and govern individual public registers, including any relevant restrictions and privacy protection mechanisms they contain. The

legality of collection and use of public register information by GCSB and NZSIS should be assessed on a case by case basis.

### **Oversight**

25. GCSB and NZSIS must carry out all activities in a manner that facilitates effective oversight. This includes keeping appropriate records of the collection of publicly available information for the purposes of fulfilling the agencies' function.

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

26. As public service agencies, GCSB and NZSIS must comply with legislation, policies and procedures common to all public service agencies.<sup>1</sup>

27. In addition, GCSB and NZSIS must have internal policies and procedures that are consistent with the requirements and principles above, and must have systems in place to support and monitor compliance. Those policies and procedures must also address the following additional matters:

- ***Compliance with the information privacy principles***

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 collecting publicly available personal information and the handling of any information collected or held as a result of such activities must incorporate guidance about compliance with the information privacy principles.

- ***Consideration of impact on rights affirmed under New Zealand Bill of Rights Act 1990***

In developing policies and procedures relating to obtaining, collecting and using publicly available information, GCSB and NZSIS must consider the impact of obtaining, collecting and using publicly available information on the rights affirmed under the New Zealand Bill of Rights Act 1990, including, as relevant, sections 14, 15, 16, 17 and 19 (manifestation of religion and belief, freedom of peaceful assembly, freedom of association, and freedom from discrimination).

- ***Sensitive category individuals***

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, Members of New Zealand's Parliament, members of the New Zealand judiciary, holders of the privileges outlined in the Intelligence and Security Act 2017, New Zealand journalists, refugees, asylum seekers and protected persons, and people vulnerable by reason of illness or other incapacity).

---

<sup>1</sup> This includes the Public Service Act 2020 and the Health and Safety at Work Act 2015.

Authorisation at a high level within the relevant agency is required for activities conducted in respect of these individuals. This will provide reassurance that appropriate measures are in place in the event that publicly available information may be obtained or used in respect of sensitive category individuals.

- **Collection of large personal datasets**

GCSB and NZSIS may collect large datasets which might include personal information relating to a number of individuals. GCSB and NZSIS must have a policy that provides guidance on the collection, use, retention and disposal of this type of information.

- **Copyright**

Collection of publicly available information by GCSB and NZSIS may raise issues about access to and use of copyrighted information. Section 63 of the Copyright Act 1994 provides that copyright is not infringed by any use of material by or on behalf of the Crown for the purpose of national security, although for any such use the Crown is liable to pay equitable remuneration to the copyright owner. In many instances, GCSB and NZSIS's collection of publicly available information will not result in a copyright infringement, however, where GCSB or NZSIS employees have concerns or uncertainty about a potential copyright infringement, they should seek legal advice.

- **Training**

All employees of an intelligence and security agency who use publicly available information collected by the NZSIS or GCSB in their work must be provided training on all relevant law, policies and procedures in relation to the collection and use of publicly available information.

#### **Authorisation procedures**

28. GCSB and NZSIS must ensure that where any difficult or sensitive issues regarding the legality or propriety of the collection and use of publicly available information arise, these are dealt with at a sufficiently senior level within the agency; the issue is escalated appropriately and where necessary expert advice, including legal advice, is sought.

#### **Duration of ministerial policy statement**

29. This MPS will take effect from XX November 2021 for a period of three years. The Minister who issued an MPS may, at any time, amend, revoke or replace the MPS.

## ATTACHMENT D

2017 version of Ministerial Policy Statement: Obtaining and Using Publicly Available Information

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982



## *Ministerial Policy Statement*

# Obtaining and using publicly available information

### **Summary**

It is lawful for the Government Communications Security Bureau (GCSB) and the New Zealand Security Intelligence Service (NZSIS) to obtain and use publicly available information. This ministerial policy statement (MPS) provides guidance on the conduct of this activity. In making decisions related to obtaining and using publicly available information, GCSB and NZSIS must have regard to the following principles: respect for privacy, necessity, proportionality, least intrusive means, respect for freedom of expression, including the right to advocate, protest or dissent, legality and oversight. This MPS also specifies certain matters to be included in internal policies and procedures.

### **Definitions**

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

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

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

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

**Publicly available information** means *information that:*

- a) *is published in printed or electronic form or broadcast;*
- b) *is generally available to members of the public free of charge or on payment of a fee;*
- c) *is included in a public register (including public registers not covered by the Privacy Act 1993).*

## Purpose

1. This MPS is issued by the Minister Responsible for the GCSB and the NZSIS pursuant to section 206(f) of the Act.
2. The purpose of this MPS is to provide guidance to GCSB and NZSIS on lawfully obtaining and using publicly available information. The MPS comprises the Minister's expectations for how GCSB and NZSIS should properly perform their functions and establishes a framework for good decision-making and best practice conduct.
3. MPSs are also relevant to oversight of the agencies by the Inspector-General of Intelligence and Security in the exercise of their propriety jurisdiction (the Act requires the Inspector-General of Intelligence and Security to take account of any relevant MPS and the extent to which an agency has had regard to it when conducting any inquiry or review).
4. Every employee making decisions or taking any action related to obtaining and using publicly available information must have regard to this MPS. Employees should be able to explain how they had regard to the MPS. This might amount to an explanation of their consideration of any relevant internal policy or procedures that reflect the MPS. The Directors-General are responsible for ensuring the MPS is reflected in their agency's internal policies and procedures. If any action or decision is taken that is inconsistent with the MPS, employees must be able to explain why the action was taken and how they had regard to the MPS.

## Scope

5. This MPS only applies to the lawful collection and use of information that is publicly available information, including publicly available personal information, by GCSB and NZSIS. A social media group that is completely open to the public or a Tweet that is broadcast to the world at large clearly contains publicly available information. Such information could be retrieved and viewed by any member of the public from their computer at any time, and people sharing such information with an unrestricted audience would not likely have a reasonable expectation of privacy with regard to the use of that information.
6. At the opposite end of the spectrum, people may share information within closed groups or to people they have proactively accepted as being able to view that shared information. Such information could not be retrieved or viewed by any member of the public at any time, because an additional step (ie, being approved by the information sharer) is required before it can be viewed. It would be reasonable for the people sharing this information to have an expectation that it would remain private within the particular group or audience and that such information is not generally available to the public. This information is beyond the scope of this MPS.
7. Information that is not publicly available may still be able to be lawfully obtained by GCSB and NZSIS, including by a person voluntarily disclosing that information or pursuant to an intelligence warrant. This MPS does not apply to obtaining or using such information. The MPS on *Collecting information lawfully from persons without an intelligence warrant or authorisation given under section 78* will be relevant to such activities. Where an authorisation has been issued in relation to such activity, it must be conducted in accordance with the terms of that authorisation, including any restrictions or conditions set out in the authorisation.
8. Similarly, this MPS does not apply to the undeclared attendance of GCSB or NZSIS employees at a public meeting, or when the agencies are conducting other forms of human intelligence or surveillance activities. The MPSs on *Collecting information lawfully from persons without an*

*intelligence warrant or authorisation given under section 78 and Surveillance in a public place* will be relevant to such activities.

## **Context**

9. GCSB's and NZSIS's objectives are set out in the Act. Both agencies contribute to:
  - a) The protection of New Zealand's national security;
  - b) The international relations and well-being of New Zealand; and
  - c) The economic well-being of New Zealand.
10. GCSB and NZSIS do this through the performance of their statutory functions, which include:
  - a) Intelligence collection and analysis; and
  - b) The provision of protective security services, advice and assistance.
11. MPSs are an important component of the measures put in place by the Act to ensure the functions of GCSB and NZSIS are performed with propriety and in accordance with New Zealand law and all human rights obligations recognised by New Zealand law.
12. GCSB and NZSIS obtain information from a range of sources to perform their intelligence collection and analysis function. Those sources include those that the agencies are able to access due to their statutory powers (for example, through the use of covert surveillance, or the interception of private communications under the authority of an intelligence warrant), and information available to any member of the public (for example, information published in the media or openly on the internet).
13. Publicly available information may lead to the production of intelligence (often referred to as 'open source intelligence'). For example, NZSIS may produce intelligence reports about threats of terrorism or violent extremism based on information available on publicly accessible forums. That information may also be used by GCSB and NZSIS to support the collection and analysis of information from other sources (for example, GCSB may research and develop methods of obtaining information through publicly available technical information).
14. The agencies also use information from a range of sources – including publicly available information and open source intelligence produced using that information – to perform their other functions. For instance, GCSB may use publicly available indicators of compromise in providing consented cyber-security activities, or NZSIS may use information published online when vetting for security clearances. Covert and specialised collection of information is both expensive and may involve intrusive powers of the State. For this reason, it is beneficial for GCSB and NZSIS to be able to meet information needs as much as possible from publicly available sources.
15. Unlike most individuals (but similar to many commercial organisations), GCSB and NZSIS may be able to obtain relatively large amounts of publicly available information without the knowledge of persons concerned (including when using an assumed identity), may analyse that information alongside information obtained from other sources, and may have sophisticated ways of analysing that information. These capabilities mean GCSB and NZSIS may be able to use publicly available information to inform assessments and/or identify details that are not immediately obvious from a piece of information considered in isolation.
16. Publicly available information may be used to corroborate, support, or provide a counter-narrative to information obtained secretly. Open source intelligence supports intelligence activity across all GCSB and NZSIS activity, including in operations, investigations, and maintaining geo-political awareness. As with information available from any source, publicly available information can be



useful in ascertaining an individual's intentions, identifying persons of concern, and eliminating individuals from investigations. Publicly available information also may form the basis of secret intelligence once assessed and combined with other intelligence sources.

## Principles

17. The following principles constitute a framework for good decision-making and must be taken into account by GCSB and NZSIS when obtaining and using publicly available information. This activity should be subject to ongoing review as to whether it continues to be consistent with these principles.

### *Respect for privacy*

18. There may be some privacy interests in publicly available information, particularly where that information is personal information. This does not preclude the agencies from accessing or using that information, but special precautions may need to be taken to protect particularly sensitive information once collected. This may include taking steps to mitigate the privacy impact of obtaining and using publicly available information, such as limiting the number of employees who may view analysis of personal information, or anonymising personal information. Importantly, GCSB and NZSIS are subject to the Privacy Act 1993 and [information privacy principles](#) 1, 4(a), and 5-12 apply where the agencies have access to personal information.
19. Obtaining publicly available personal information will activate the obligation under privacy principle 8 (accuracy, etc, of personal information to be checked before use). GCSB and NZSIS must take steps that are reasonable in the circumstances to ensure that the information is accurate, up to date, complete, relevant and not misleading (having regards to the purpose for which the information is proposed to be used) before using that information. This is relevant, for example, in performing the NZSIS's security vetting function.
20. The public register privacy principles within section 59 of the Privacy Act 1993 will be relevant to the manner in which GCSB and NZSIS seek to gain information from public registers.

### *Necessity*

21. Publicly available information, including personal information, should only be obtained and used for a purpose that is consistent with GCSB and NZSIS performing their statutory functions. GCSB and NZSIS should be clear that any activities involving the collection of publicly available information have a clear purpose, and ensure the purpose continues to remain throughout the course of the collection activities.
22. Examples of purposes where it will be necessary to obtain and use publicly available information include acquiring background or contextual information relevant to the performance of a statutory function, acquiring information to identify behavioural patterns of interest, and obtaining information to assess the accuracy of information already held.
23. Collecting information for the personal interest of an employee (unrelated to their role) while acting in their official capacity, for example, would not satisfy the necessity principle.

### *Proportionality*

24. The collection and use of publicly available information should be proportionate to the purpose for which it is carried out. The amount of information may be one factor to consider when assessing proportionality. For example, bulk collection of publicly available information should

only be carried out where this is proportionate to the purpose. The age of information may also be a consideration, as there may be an increased risk that the information is out of date and less likely to be fit for purpose.

25. Publicly available information may be collected and used to identify associates or contacts of a person of security concern. Publicly available information and analysis carried out using that information may contain personal or sensitive information about individuals not relevant to the purpose for which information is sought. Where practicable, GCSB and NZSIS should minimise the collection of publicly available personal information about persons who are not relevant to the purpose for which information is sought.
26. When publicly available personal information is collected, assessed, collated and combined across multiple sources, GCSB and NZSIS should assess the additional privacy impact of collection from each additional source. When considered with the least intrusive means principle below, this places some bounds on the collection of publicly available personal information.
27. Privacy principles 10(a) and 11(b) place limits on using and disclosing personal information sourced from a publicly available publication where it would be unfair or unreasonable to do so, unless there is reasonable grounds to believe the use or disclosure is necessary to enable GCSB or NZSIS to perform any of its functions (privacy principles 10(2) and 11 (fa)). Fairness and reasonableness are therefore important tests when making a proportionality assessment.

#### *Least intrusive means*

28. In collecting publicly available information, GCSB and NZSIS must use the least intrusive means available to obtain the required information in a secure, timely and reliable manner (noting that open source collection is one of the least intrusive means of collection of intelligence, especially compared to warranted methods).

#### *Respect for freedom of expression, including the right to advocate, protest, or dissent*

29. Section 19 of the Act provides that the exercise by any person in New Zealand or any class of persons in New Zealand of their right to freedom of expression under the law (including the right to advocate, protest, or dissent) does not itself justify an intelligence and security agency taking any action in respect of that person or class of persons.
30. GCSB and NZSIS must ensure that its use of particular information sources or platforms to obtain publicly available information is consistent with the protection in section 19. Acts of advocacy, protest or dissent are not, of themselves, justification for collecting publicly available information. GCSB and NZSIS must ensure collection of publicly available information related to such acts is undertaken only where the purpose of doing so is necessary to enable the agency to perform one of its statutory functions in furtherance of one (or more) of its objectives. For example, the fact of a protest itself is not sufficient justification for collecting information but following up on a legitimate security concern that arises in relation to a planned protest may be sufficient justification.

#### *Legality*

31. GCSB and NZSIS must ensure that the collection and use of publicly available information will be carried out in accordance with the law. Where appropriate, legal advice should be sought. As noted above, particular care must be taken to ensure that, without a warrant or using other

methods recognised under the Act, only information that is publicly available is collected by GCSB and NZSIS.

32. GCSB and NZSIS may collect publicly available information using collection methods that are not available to the public (for example, by using specialist techniques for collecting information or through relationships with other people who have access to the information). The agencies must take particular care to ensure that any collection of publicly available information using methods not available to the public does not involve any unlawful activity, unless done so with an authorisation under Part 4 of the Act.
33. In addition to complying with the law, GCSB and NZSIS must consider the impact of obtaining and using publicly available information on the rights affirmed under sections 15 (manifestation of religion and belief), 16 (freedom of peaceful assembly), 17 (freedom of association) and 19 (freedom from discrimination) of the New Zealand Bill of Rights Act 1990.
34. GCSB and NZSIS must have regard to the statutes that establish and govern individual public registers, including any relevant restrictions and privacy protection mechanisms they contain. The legality of collection and use of public register information by GCSB and NZSIS should be assessed on a case by case basis.

#### *Oversight*

35. GCSB and NZSIS must carry out all activities in a manner that facilitates effective oversight, including through the keeping of appropriate records of collection of publicly available information made in respect of particular individuals.

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

36. GCSB and NZSIS must have internal policies and procedures that are consistent with the requirements and principles above, and must have systems in place to support and monitor compliance. Those policies and procedures must also address the following additional matters:

##### **Compliance with the information privacy principles**

GCSB and NZSIS are subject to information privacy principles 1, 4(a), and 5 to 12 of the [information privacy principles](#) in the Privacy Act 1993. All policies relating to obtaining publicly available personal information and the handling of any information collected or held as a result of such activities must incorporate guidance about compliance with the information privacy principles.

##### **Compliance with public service minimum standards of integrity and conduct**

The Directors-General of the GCSB and NZSIS must issue policies and procedures that reflect their agencies' obligations under the Public Service Act 2020.

##### **Health and safety**

The collection and use of publicly available information must be undertaken consistently with GCSB's and NZSIS's obligations under the Health and Safety at Work Act 2015.

##### **Sensitive category individuals**

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, Members of New Zealand's Parliament, members of the New Zealand judiciary, journalists, lawyers, registered medical practitioners or other providers

of health services attracting medical privilege, and people vulnerable by reason of illness or other capacity).

Authorisation at a high level within the relevant agency is required for activities conducted in respect of these individuals. This will provide reassurance that appropriate measures are in place in the event that publicly available information may be obtained or used in respect of sensitive category individuals.

### **Copyright**

Collection of publicly available information by GCSB and NZSIS may raise issues about access to and use of copyrighted information. Section 63 of the Copyright Act 1994 provides that copyright is not infringed by any use of material by or on behalf of the Crown for the purpose of national security, although for any such use the Crown is liable to pay equitable remuneration to the copyright owner.

GCSB and NZSIS should have a policy that provides guidance to employees about the issues raised by copyright in publicly available information to ensure that the Crown's legal obligations are met.

### **Training**

All employees of an intelligence and security agency who use publicly available information in their work must be provided training on all relevant law, policies and procedures in relation to the collection and use of publicly available information.

## **Authorisation procedures**

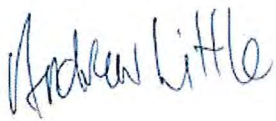
37. GCSB and NZSIS must ensure that where any difficult or sensitive issues regarding the legality or propriety of the collection and use of publicly available information arise, these are dealt with at a sufficiently senior level within the agency. For example, publicly available information may include information that has been previously leaked from or mislaid by its owner. In situations where this is known or suspected to have occurred, employees must ensure that the issue is escalated appropriately and where necessary expert advice, including legal advice, is sought.

### **Duration of ministerial policy statement**

38. This MPS will take effect from 28 September 2020 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

September 2020

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

# ATTACHMENT E

Draft revised Ministerial Policy Statement: Section 121 requests

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982



## *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

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

**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 in [LINK])
  - iv. from overseas public authorities (guidance on cooperation with overseas public authorities is addressed in [LINK])
- b. Obtaining, collecting and using publicly available information [LINK])
- c. Through the conduct of other lawful activities, such as conducting surveillance in a public place [LINK].

#### **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 (i.e. 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 Ministerial guidance on Co-operation with Overseas Public Authorities should be considered [LINK].
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) [LINK];
  - c. are made by the GCSB to facilitate the provision of consented information assurance and cybersecurity activities under section 11 of the Act [LINK]; 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. 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 information 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***

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**

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**

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 [LINK] applies in relation to management of this information.

- **Compliance with information privacy principles**

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**

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).

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**

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**

34. 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**

35. This MPS will take effect from XX November 2021 for a period of three years. The Minister who issued a MPS may, at any time, amend, revoke or replace the MPS.

## ATTACHMENT F

2017 version of Ministerial Policy Statement: Requesting Information from agencies under section 121 of the Intelligence and Security Act 2017

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982



## *Ministerial Policy Statement*

# Requesting information from agencies under section 121 of the Intelligence and Security Act 2017

### **Summary**

The Intelligence and Security Act 2017 expressly recognises the existing ability of the Government Communications Security Bureau (GCSB) and New Zealand Security Intelligence Service (NZSIS) to request information from an agency under section 121. This ministerial policy statement (MPS) provides guidance about making those requests. In making these requests GCSB and NZSIS must have regard to the following principles: legality, 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

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

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

## Purpose

1. This MPS is issued by the Minister Responsible for the GCSB and the NZSIS pursuant to section 206(g) of the Act.
2. The purpose of this MPS is to provide guidance to GCSB and NZSIS about making requests for information under section 121 of the Act. The MPS comprises the Minister's expectations for how GCSB and NZSIS should properly perform their functions and establishes a framework for good decision-making and best practice conduct.
3. MPSs are also relevant to oversight of the agencies by the Inspector-General of Intelligence and Security in the exercise of their propriety jurisdiction (the Act requires the Inspector-General to take account of any relevant MPS and the extent to which an agency has had regard to it when conducting any inquiry or review).
4. Every employee making a request for information under section 121 must have regard to this MPS. Employees should be able to explain how they had regard to the MPS. This might amount to an explanation of their consideration of any relevant internal policy or procedures that reflect the MPS. The Directors-General are responsible for ensuring the MPS is reflected in their agency's internal policies and procedures. If any action or decision is taken that is inconsistent with the MPS, employees must be able to explain why the action was taken and how they had regard to the MPS.

## Scope

5. This MPS applies to formal requests under section 121 of the Act for information from other agencies that is necessary for the performance of GCSB's and NZSIS's functions. Corresponding disclosures by other organisations are made under section 122.
6. This MPS does not apply to information obtained under any of the other mechanisms available under the Act (discussed in more detail below), or pursuant to an intelligence warrant. Any requirements associated with obtaining information under such mechanisms or pursuant to intelligence warrants will be specifically stated in those mechanisms/intelligence warrants. Nor does it apply to informal requests for information that GCSB or NZSIS employees may make in the course of interactions with agencies (for example, requests arising in the context of a conversation or at a conference).
7. Because section 121 requires a statement from the relevant Director-General that the requested information is necessary to enable the performance of one or more of GCSB's/NZSIS's functions (see below), section 121 only applies to overt or declared requests. The agencies cannot use section 121 to make covert or undeclared requests; depending on the circumstances, such requests may constitute lawful human intelligence activities (see MPS on *Collecting information lawfully from persons without an intelligence warrant or authorisation given under section 78*).
8. New Zealand obtains a significant amount of information (including intelligence) from overseas public authorities. Cooperation and sharing of intelligence with overseas public authorities is addressed by a separate MPS (see MPS on *Cooperation with overseas public authorities*); requests for such information are not covered by this MPS.



## Context

9. GCSB's and NZSIS's objectives are set out in the Act. GCSB and NZSIS contribute to:
  - a) The protection of New Zealand's national security;
  - b) The international relations and well-being of New Zealand; and
  - c) The economic well-being of New Zealand.
10. GCSB and NZSIS do this through the performance of their statutory functions, which include:
  - a) Intelligence collection and analysis; and
  - b) The provision of protective security services, advice and assistance.
11. MPSs are an important component of the measures put in place by the Act to ensure the functions of GCSB and NZSIS are performed with propriety and in accordance with New Zealand law and all human rights obligations recognised by New Zealand law.
12. To perform any of their statutory functions, it is necessary for GCSB and NZSIS to use a range of methods to collect information, including requests for information to a range of agencies. Information (such as someone's address, information about their family and friend groups, or travel movements) may help GCSB and NZSIS to investigate the activities of that person. It may also help to verify information obtained from other sources to assess the quality of those other sources, or identify links between persons of intelligence interest. GCSB and NZSIS may request technical information (such as information about the configuration of computer networks) to provide advice and assistance to support the protection of those networks from malicious cyber activity.
13. The Act contains a range of mechanisms that, depending on the circumstances, can be used by GCSB or NZSIS to obtain information needed to perform their statutory functions:
  - Subpart 2 of Part 5 provides for direct access to certain government databases (subject to a direct access agreement between Ministers). Those databases contain, for example, information about citizenship, residency and travel movements, and financial intelligence.
  - Subpart 3 of Part 5 provides for case-by-case disclosure of certain restricted information (ie, information that cannot currently be disclosed due to a statutory prohibition or restriction). That information includes, for example, adoption information, tax information, and driver licence photographs.
  - Subpart 4 of Part 5 establishes a scheme for the compulsory disclosure of certain business records held by telecommunications companies and financial service providers.
14. GCSB and NZSIS can also obtain information through otherwise unlawful means (for example, by intercepting private communications) pursuant to an intelligence warrant. Those means are not covered by this MPS.

### *Legislative basis of requests for information*

15. Section 121 of the Act recognises the existing ability of GCSB and NZSIS to request information held by other agencies (both public and private). Section 122 recognises the existing ability of an agency to disclose information it holds to the GCSB and NZSIS (see sections 121 and 122).
16. Section 121 sets out the ability to request information from another agency where the Director-General of GCSB or NZSIS believes on reasonable grounds that the information is necessary to enable his or her agency to perform any of its functions. Such a request must provide details of

the information requested and confirm the information is necessary to enable GCSB or NZSIS to perform any of its functions. That is, the intention is that section 121 deals with overt and declared requests for information.

17. Disclosing agencies retain the discretion to decide whether to disclose information to the agencies upon receiving such a request from GCSB or NZSIS. Section 122 of the Act states organisations may disclose information if they have reasonable grounds to believe disclosure is necessary to enable the intelligence and security agency to perform any of its functions. Disclosures of information under section 122 may not be made if there are other Acts that prohibit or restrict 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. Disclosures of information also remain subject to any other obligations of confidence, or contracts, agreements or other documents relating to the disclosure of the specific information.
18. The disclosure of personal information is also subject to the Privacy Act 1993. [Information privacy principles](#) 1, 4(a), and 5 to 12 apply to GCSB and NZSIS. Information privacy principle 11 provides that an agency may disclose information if that disclosure is one of the purposes in connection with which the information was obtained or is directly related to those purposes. An exception to information privacy principle 11 permits disclosure where it is necessary to enable an intelligence and security agency to perform any of its functions (see information privacy principle 11(fa)). Depending on the information in question, it may be that industry or sector-specific privacy codes also apply (the Health Information Privacy Code 1994, for example). Even when a disclosure is consistent with information privacy principle 11, the requirements of section 122 must also be met, that is, including that the disclosing organisation must believe on reasonable grounds the disclosure is necessary to enable either GCSB or NZSIS to perform any of its functions.
19. In situations where an organisation considering disclosing information does not have reasonable grounds for believing disclosure is necessary for the performance of a function of GCSB or NZSIS, the relevant Director-General may certify that disclosure of the information is necessary to enable the agency to perform its functions (section 122(3)). Certificates will always be provided in written form.

## Principles

20. 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 section 121 of the Act. All requests for information (to the extent they are ongoing or repeated) should be subject to ongoing review as to whether they continue to be consistent with these principles.

### *Legality*

21. GCSB and NZSIS must ensure all requests made under section 121 are made in accordance with the law. Requests must be identifiable as a non-enforceable request, rather than a demand with which the recipient is legally required to comply. Where appropriate, legal advice should be sought before requests are made.

### *Necessity*

22. Requests should only be made when the information sought is necessary to enable GCSB or NZSIS to perform one or more of its functions. This reflects the law in relation to personal information – [information privacy principle 1](#) of the Privacy Act 1993 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.

23. Requests must be formulated so that they target the information that is necessary and do not seek to capture irrelevant information. Consideration of necessity will also require consideration of whether there is another way to obtain the information (for example, by directly accessing it where it falls within the direct access scheme in the Act and where a direct access agreement is in place in respect of that category of information).

#### *Proportionality*

24. The nature and amount of information requested should be proportionate to the purpose for which the information is sought. For example, a request for a larger amount of information, relating to a larger number of people, or relating to sensitive personal (for example, health information) or commercial matters, should only be made where the purpose for obtaining that information is proportionately important – such as if it will support the production of higher-priority intelligence, or is part of addressing an immediate threat. Similarly, a proportionality assessment should be made in relation to any ongoing or repeated requests for information made in reliance on section 121.

#### *Respect for privacy*

25. GCSB and NZSIS are subject to the Privacy Act 1993 and [information privacy principles](#) 1, 4(a), and 5 to 12 will apply where they have access to personal information. GCSB and NZSIS should take special care in relation to any personal information that the person who is the subject of the request has a reasonable expectation of privacy in relation to. Whether a reasonable expectation of privacy exists requires consideration of all of the circumstances, including such factors as 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. Reasonable expectations of privacy exist to protect information that would tend to reveal intimate details of the lifestyle and personal choices of the individual concerned.
26. 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 agencies, and only disclosing that information where there is a legitimate need.
27. 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. Legal advice should be sought in such cases.

#### *Less intrusive means to be considered*

28. GCSB and NZSIS should seek to obtain any information by the least intrusive means reasonably available. This means GCSB and NZSIS should only make a request for information where a less intrusive means of obtaining the information is not reasonably available. A request for information is a reasonably available means of obtaining information and is preferable to more intrusive means of obtaining the information.

29. The intrusiveness of requests for information vary according to the particular information requested. While requests for information from other agencies are often less intrusive than other methods of collection (for example, warranted methods) for the agency receiving the request, 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.
30. Generally, 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, other persons who are aware of their financial situation, and their bank.

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

31. Generally, the Act is designed to operate as a toolkit from which the agencies may utilise any appropriate mechanism for obtaining information. For example, section 155 makes clear that nothing in the business records authorisation regime in the Act precludes the disclosure of business records to GCSB and NZSIS where disclosure is required, authorised or permitted by or under another provision of the Act or any other statute.
32. Where the Act or another enactment provides a specific mechanism (other than an authorisation under Part 4 of the Act) for access by GCSB/NZSIS to 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 will generally provide greater protection for individual privacy interests than case by case requests. 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, the agencies should use that mechanism instead of making ad-hoc requests under section 121. It is important to note, however, that the existence of a specific scheme does not preclude GCSB and NZSIS from making ad-hoc requests under section 121 if there are operational reasons to do so (such as urgent requests).

#### *Oversight*

33. GCSB and NZSIS must carry out all activities in a manner that facilitates effective oversight, including through the keeping of records about requests for information. These records should include enough information to allow a person reviewing a request to identify the purpose for making that request.
34. 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 under section 123.
35. GCSB and NZSIS should record the response to each request (ie, request fulfilled entirely, request fulfilled partially, or request denied) to allow for transparency reporting about the number of requests for information under section 121.

## Matters to be reflected in internal policies and procedures

36. GCSB and NZSIS must have, and act in compliance with, internal policies and procedures that are consistent with the requirements and principles above, and must have systems in place to support and monitor compliance. The policies and procedures of GCSB and NZSIS must also address the following specific matters.

### Compliance with the State Services Code of Conduct

The Directors-General of GCSB and NZSIS must issue policies and procedures that reflect their agencies' obligations under the State Sector Act 1988.

Consistent with the State Services [Standards of Integrity and Conduct](#), the agencies will not permit individual employees to request information about any person or matter that they have a personal interest in or relationship (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.

### Training

GCSB and NZSIS employees may only make requests for information 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

Information received as the result of a request from agencies under 121 may be among some of the more sensitive information held by GCSB and NZSIS, given the personal nature of that information. This information must be handled and stored in accordance with clear access controls that correspond to the sensitivity of the information. The MPS [link management of information] also applies in relation to management of this information.

### Compliance with information privacy principles

GCSB and NZSIS are subject to [information privacy principles](#) 1, 4(a), and 5 to 12 of the information privacy principles in the Privacy Act 1993. All policies relating to requests made under section 121 of the Act and the handling of any information collected and held as a result of such requests must incorporate guidance about compliance with the relevant information privacy principles.

### Sensitive category individuals

GCSB and NZSIS must have a policy setting out how 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, Members of New Zealand's Parliament, members of the New Zealand judiciary, journalists, lawyers, registered medical practitioners or other providers of health services attracting medical privilege, and people vulnerable by reason of illness or other incapacity).

Authorisation at a high level within the relevant agency 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.

### **Authorisation procedures**

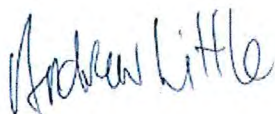
37. The Directors-General of GCSB and NZSIS may delegate their ability to make requests for information consistently with the Public Service Act 2020.
38. All requests for information must be authorised by an appropriately senior employee of the agencies, having regard to the nature of the information requested and the agency it is requested from (such as sensitive categories of individuals), and any risks associated with making the request.

### **Duration of ministerial policy statement**

39. This MPS will take effect from 28 September 2020 for a period of three years. The Minister who issued a 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

September 2020

# ATTACHMENT G

## Letter to Hon Kris Faafoi, Minister of Justice

Hon Kris Faafoi  
Minister of Justice  
Parliament Buildings

Dear Minister Faafoi

### Consultation on Ministerial Policy Statement – Publicly Available Information

I enclose for your comment a draft of the revised Ministerial Policy Statement (MPS) regarding GCSB and NZSIS collecting and using publicly available information.

Sections 206 and 207 of the Intelligence and Security Act (the Act) require the Minister(s) responsible for the intelligence and security agencies to issue MPSs about certain lawful activities carried out by the agencies. The MPSs are required to be reviewed within three years from the date they take effect.

MPSs are a mechanism for the responsible Minister(s) to set expectations and provide guidance about the conduct of those activities. MPSs do not affect the lawfulness of the activities, but must be taken into account by the Inspector-General of Intelligence and Security when they are assessing the propriety of the agencies' activities. As the current Minister responsible for both the GCSB and the NZSIS, I must review and reissue the MPSs.

Under section 212 of the Act I am required to consult with any Ministers of the Crown whose area of responsibility includes an interest in the proposed statement. In this case, I seek your comments, as this MPS is relevant to your portfolio responsibilities as Minister of Justice. I have outlined the main changes to this MPS below.

I would welcome any insights that you may have. Officials from the Department of the Prime Minister and Cabinet have liaised with officials from the Ministry of Justice and their feedback has been incorporated in the attached draft.

If you have any comments, I would be grateful to receive these by **[date]**.

Yours sincerely

Hon Andrew Little  
**Minister Responsible for the GCSB**  
**Minister Responsible for the NZSIS**

## Key changes to the attached Ministerial Policy Statement

---

### Changes common to all eleven MPSs

All MPSs have been amended to:

- Include a cover sheet (or website landing page). The cover sheet sets out the overarching purpose of the MPSs, so each individual MPS just focuses on the specific activity in covers;
- Improve readability, by simplifying the language (including the titles of the MPSs) and reducing repetition;
- Separate the context (which is of more interest to the public) and the guidance to the agencies;
- Clarify that the MPS only applies to lawful activity, and set out the legal obligations in relation to the activity covered by the MPS;
- Set out that the agencies are public service agencies and must comply with policies and procedures common to all New Zealand public service agencies.

### Changes consistent across the information collection MPSs

The Publicly Available Information was reviewed alongside the other information collection MPSs (Collecting Human Intelligence and Section 121 Requests). These MPSs now include a description of the information collection framework – setting out the methods the agencies use to perform their statutory functions, and revising the scope sections to clearly specify what is in scope of each MPS, what is out of scope and what is in scope of another MPS. This is as the result of feedback that GCSB and NZSIS employees were sometimes confused about which MPS applied to which activity.

### Changes to the Publicly Available Information MPS

The *Publicly Available Information MPS* sets out my expectations on how GCSB and NZSIS properly obtain, collect and use publicly available information.

The main feedback on this MPS was that the MPS was focused on the use of publicly available information in relation to specific persons of interest. The revised MPS has been re-framed to capture the broader range of uses of publicly available information. The range of uses have been described. Other changes include:

- The MPS now includes a requirement that the agencies have an internal policy that provides guidance on the collection, use, retention and disposal of large personal datasets that were obtained through collecting publicly available information;
- It includes an example to demonstrates the applicability of section 19 of the Act (which provides that the exercise of the right to freedom of expression does not justify activity by an intelligence and security agency) in relation to publicly available information.



# ATTACHMENT H

## Letter to Hon Dr David Clark, Minister for Digital Economy and Communications

Hon Dr David Clark  
Minister for Digital Economy and Communications  
Parliament Buildings

Dear Minister Clark

### Consultation on Ministerial Policy Statement – Publicly Available Information

I enclose for your comment a draft of the revised Ministerial Policy Statement (MPS) regarding GCSB and NZSIS collecting and using publicly available information.

Sections 206 and 207 of the Intelligence and Security Act (the Act) require the Minister(s) responsible for the intelligence and security agencies to issue MPSs about certain lawful activities carried out by the agencies. The MPSs are required to be reviewed within three years from the date they take effect.

MPSs are a mechanism for the responsible Minister(s) to set expectations and provide guidance about the conduct of those activities. MPSs do not affect the lawfulness of the activities, but must be taken into account by the Inspector-General of Intelligence and Security when they are assessing the propriety of the agencies' activities. As the current Minister responsible for both the GCSB and the NZSIS, I must review and reissue the MPSs.

Under section 212 of the Act I am required to consult with any Ministers of the Crown whose area of responsibility includes an interest in the proposed statement. In this case, I seek your comments, as this MPS is relevant to your portfolio responsibilities as Minister for Digital Economy and Communications. I have outlined the main changes to this MPS below.

I would welcome any insights that you may have. Officials from the Department of the Prime Minister and Cabinet have consulted with the Government Chief Privacy Officer and his feedback has been incorporated in the attached draft.

If you have any comments, I would be grateful to receive these by **[date]**.

Yours sincerely

Hon Andrew Little  
**Minister Responsible for the GCSB**  
**Minister Responsible for the NZSIS**

## Key changes to the attached Ministerial Policy Statement

---

### Changes common to all eleven MPSs

All MPSs have been amended to:

- Include a cover sheet (or website landing page). The cover sheet sets out the overarching purpose of the MPSs, so each individual MPS just focuses on the specific activity in covers;
- Improve readability, by simplifying the language (including the titles of the MPSs) and reducing repetition;
- Separate the context (which is of more interest to the public) and the guidance to the agencies;
- Clarify that the MPS only applies to lawful activity, and set out the legal obligations in relation to the activity covered by the MPS;
- Set out that the agencies are public service agencies and must comply with policies and procedures common to all New Zealand public service agencies.

### Changes consistent across the information collection MPSs

The Publicly Available Information was reviewed alongside the other information collection MPSs (Collecting Human Intelligence and Section 121 Requests). These MPSs now include a description of the information collection framework – setting out the methods the agencies use to perform their statutory functions, and revising the scope sections to clearly specify what is in scope of each MPS, what is out of scope and what is in scope of another MPS. This is as the result of feedback that GCSB and NZSIS employees were sometimes confused about which MPS applied to which activity.

### Changes to the Publicly Available Information MPS

The *Publicly Available Information MPS* sets out my expectations on how GCSB and NZSIS properly obtain, collect and use publicly available information.

The main feedback on this MPS was that the MPS was focused on the use of publicly available information in relation to specific persons of interest. The revised MPS has been re-framed to capture the broader range of uses of publicly available information. The range of uses have been described. Other changes include:

- The MPS now includes a requirement that the agencies have an internal policy that provides guidance on the collection, use, retention and disposal of large personal datasets that were obtained through collecting publicly available information;
- It includes an example to demonstrate the applicability of section 19 of the Act (which provides that the exercise of the right to freedom of expression does not justify activity by an intelligence and security agency) in relation to publicly available information.

# ATTACHMENT I

## Letter to Hon Poto Williams, Minister of Police

Hon Poto Williams  
Minister of Police  
Parliament Buildings

Dear Minister Williams

### Consultation on Ministerial Policy Statements – Human Intelligence, Section 121 Requests, and Publicly Available Information

I enclose for your comment drafts of three revised Ministerial Policy Statements (MPSs) that provide guidance to the GCSB and NZSIS on information collection. They are:

- Collecting Human Intelligence
- Publicly Available Information
- Section 121 Requests.

Sections 206 and 207 of the Intelligence and Security Act (the Act) require the Minister(s) responsible for the intelligence and security agencies to issue MPSs about certain lawful activities carried out by the agencies. The MPSs are required to be reviewed within three years from the date they take effect.

MPSs are a mechanism for the responsible Minister(s) to set expectations and provide guidance about the conduct of those activities. MPSs do not affect the lawfulness of the activities, but must be taken into account by the Inspector-General of Intelligence and Security when they are assessing the propriety of the agencies' activities. As the current Minister responsible for both the GCSB and the NZSIS, I must review and reissue the MPSs.

Under section 212 of the Act I am required to consult with any Ministers of the Crown whose area of responsibility includes an interest in the proposed statement. In this case, I seek your comments, as these MPSs are relevant to your portfolio responsibilities as Minister of Police. I have outlined the main changes to these MPSs below.

Given your portfolio responsibilities for New Zealand Police, who undertake similar activities, I would welcome any insights that you may have. Officials from the Department of the Prime Minister and Cabinet have liaised with officials from New Zealand Police and their feedback has been incorporated in the attached draft. I understand that New Zealand Police has also provided comments on specific operational guidance which the GCSB and NZSIS will incorporate in their internal operational guidance on these activities.

If you have any comments, I would be grateful to receive these by **[date]**.

Yours sincerely

Hon Andrew Little  
**Minister Responsible for the GCSB**  
**Minister Responsible for the NZSIS**

## Key changes to the attached Ministerial Policy Statements

---

### Changes common to all eleven MPSs

All MPSs have been amended to:

- Include a cover sheet (or website landing page). The cover sheet sets out the overarching purpose of the MPSs, so each individual MPS just focuses on the specific activity in covers;
- Improve readability, by simplifying the language (including the titles of the MPSs) and reducing repetition;
- Separate the context (which is of more interest to the public) and the guidance to the agencies;
- Clarify that the MPS only applies to lawful activity, and set out the legal obligations in relation to the activity covered by the MPS;
- Set out that the agencies are public service agencies and must comply with policies and procedures common to all New Zealand public service agencies.

### Changes consistent across the information collection MPSs

The MPSs now include a description of the information collection framework – setting out the methods the agencies use to perform their statutory functions, and revising the scope sections to clearly specify what is in scope of each MPS, what is out of scope and what is in scope of another MPS. This is as the result of feedback that GCSB and NZSIS employees were sometimes confused about which MPS applied to which activity.

### Changes to the Collecting Human Intelligence MPS

The *Collecting Human Intelligence MPS* sets out my expectations, as responsible Minister, for how GCSB and NZSIS properly collect information from individuals (referred to as human intelligence) without an intelligence warrant or authorisation under the Act.

The main changes to this MPS are:

- The context section has been made clearer and has been simplified;
- The 'warnings' section has been revised to provide more guidance to the agencies on how to make a statement to people they engage with that is intended to deter a person from a particular course of action. The MPS now stipulates that the agencies must have an internal policy to guide this activity;
- A separate 'conflicts of interest' section has been added, to be clear that employees should not be involved in operations where a conflict of interest exists;
- It now specifies that foreign implications may arise in relation to domestic human intelligence activity, and in these circumstances the agencies must consult MFAT.

### Changes to the Publicly Available Information MPS

The *Publicly Available Information MPS* sets out my expectations on how GCSB and NZSIS properly obtain, collect and use publicly available information.

The main feedback on this MPS was that the MPS was focused on the use of publicly available information in relation to specific persons of interest. The revised MPS has been re-framed to

capture the broader range of uses of publicly available information. The range of uses have been described. Other changes include:

- The MPS now includes a requirement that the agencies have an internal policy that provides guidance on the collection, use, retention and disposal of large personal datasets that were obtained through collecting publicly available information;
- It includes an example to demonstrate the applicability of section 19 of the Act (which provides that the exercise of the right to freedom of expression does not justify activity by an intelligence and security agency) in relation to publicly available information.

### **Changes to the Section 121 Requests MPS**

The *Section 121 Requests MPS* sets out my expectations for how the agencies make requests under section 121 of the Act.

The main changes to this MPS are:

- It now clarifies the scope of a section 121 request. The previous MPS used the term 'formal requests', which was not clear to operational staff. The revised MPS includes more information about what is in and out of scope;
- It has been revised to make it clear that section 121 requests can include requests for information to assess the validity of leads;
- The oversight section now sets out that the way in which section 121 requests are recorded may depend on the request (including a saved email).