



Ref: OIA-2021/22-1127

Dear [REDACTED]

**Official Information Act request relating to GCSB-NZSIS Ministerial Policy Statement briefings**

Thank you for your Official Information Act 1982 (the Act) request received on 16 March 2022. You requested:

- “ONE: “Review of the Ministerial Policy Statements under the Intelligence and Security Act 2017” [1920NSP/010]*  
*TWO: “Review of the Overseas Cooperation Ministerial Policy Statement: Proposed Consultation Plan” [1920NSP/031]*  
*THREE: “Proposed Revised Approach for Reviewing the Ministerial Policy Statements” [1920NSP/081]*  
*FOUR: “Consultation on Ministerial Policy Statement: Conducting surveillance in a public place” [1920NSP/054]*  
*FIVE: “Review of the Ministerial Policy Statements - revised timing” [2021NSP/010]*  
*SIX: “Consultation on ministerial policy statement: cooperating with overseas public authorities” [2021NSP/030]*  
*SEVEN: “Ministerial Policy Statement: Cooperating with overseas public authorities - approval to reissue” [2021NSP/066]*  
*EIGHT: “Consultation on three Ministerial Policy Statements” [2021NSP/086]*  
*NINE: “Consultation on Ministerial Policy Statement: Information Assurance and Cybersecurity Activities” [02 Jul 2021]*  
*TEN: “Consultation on Ministerial Policy Statement: Information Management” [05 Jul 2021]*  
*ELEVEN: “Consultation on the final three reviewed Ministerial Policy Statements” [27 Oct 2021]”*

I have decided to release the documents listed below, subject to information being withheld as noted. The relevant grounds under which information has been withheld are:

- section 6(a) – the making available of the information would be likely to prejudice the security or defence of New Zealand or the international relations of the Government of New Zealand;
- section 9(2)(a) – the withholding of the information is necessary to protect the privacy of natural persons.

Item	Date	Document Title
1.	27 September 2019	Review of the Ministerial Policy Statements under the Intelligence and Security Act 2017
2.	24 January 2020	Review of the Ministerial Policy Statements Update and Proposed Consultation Plan

3.	21 June 2020	Briefing: Proposed Revised Approach for Reviewing the Ministerial Policy Statements
4.	22 June 2020	Consultation on Ministerial Policy Statement: Conducting Surveillance in a Public Place
5.	28 August 2020	Review of the Ministerial Policy Statements – Revised Timing
6.	18 December 2020	Consultation on Ministerial Policy Statement: Cooperating with Overseas Public Authorities
7.	12 March 2021	Briefing: Ministerial Policy Statement: Cooperating with Overseas Public Authorities – Approval to Reissue
8.	8 April 2021	Briefing: Consultation on Three Ministerial Policy Statements
9.	2 July 2021	Consultation on Ministerial Policy Statement: Information Assurance and Cybersecurity Activities
10.	5 July 2021	Briefing: Consultation on Ministerial Policy Statement: Information Management
11.	27 October 2021	Briefing: Consultation on the Final Three Reviewed Ministerial Policy Statements

In making my decision, I have taken the public interest considerations in section 9(1) of the Act into account.

You have the right to ask the Ombudsman to investigate and review my decision under section 28(3) of the Act.

This response will be published on the Department of the Prime Minister and Cabinet's website during our regular publication cycle. Typically, information is released monthly, or as otherwise determined. Your personal information including name and contact details will be removed for publication.

Yours sincerely

p.p.  
Tony Lynch  
**Deputy Chief Executive**  
**National Security Group**



# Briefing

## REVIEW OF THE MINISTERIAL POLICY STATEMENTS UNDER THE INTELLIGENCE AND SECURITY ACT 2017

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

Date	27/09/2019	Priority	Routine
Deadline	n/a	Briefing Number	1920NSP/010

### Purpose

This briefing:

- Sets out the context and background to reviewing the ministerial policy statements, as required under the Intelligence and Security Act 2017
- Seeks your agreement to the proposed approach for reviewing the ministerial policy statements
- Discusses the proposed review of the overseas cooperation ministerial policy statement.

### Recommendations

1. **Note** that the ministerial policy statements are required to be reviewed before September 2020
2. **Agree** that the Department of the Prime Minister and Cabinet undertakes the reviews of the ministerial policy statements on your behalf **YES / NO**
3. **Agree** that the approach to reviewing the ministerial policy statements is the same as the approach taken to developing the ministerial policy statements in 2017 (paragraph 6) **YES / NO**
4. **Note** that the recently released Inspector-General of Intelligence and Security's report of her inquiry into possible New Zealand engagement with the CIA detention programme recommended an early review of the overseas cooperation ministerial policy statement
5. **Indicate** whether you wish to consult with relevant NGOs on the review of the overseas cooperation ministerial policy statement **YES / NO**

6. **Indicate** whether you would like to discuss the proposed review of the ministerial policy statements with officials from the Department of the Prime Minister and Cabinet. **YES / NO**

		
Tony Lynch Deputy Chief Executive National Security Group		Hon Andrew Little Minister Responsible for the GCSB and NZSIS
26/09/2019		...../...../2019

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

Contact for telephone discussion if required:

Name	Position	Telephone	1st contact
Pip Swaney	Team 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

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

# REVIEW OF THE MINISTERIAL POLICY STATEMENTS UNDER THE INTELLIGENCE AND SECURITY ACT 2017

## Purpose

---

1. This briefing:
  - Sets out the context and background to reviewing the ministerial policy statements
  - Seeks your agreement to the proposed approach for reviewing the ministerial policy statements
  - Discusses the proposed review of the overseas cooperation ministerial policy statement.

## What are the ministerial policy statements?

---

2. Ministerial policy statements (MPSs) are required under section 206 and section 207 of the Intelligence and Security Act 2017 (the Act) to set out the responsible Minister's expectations of the GCSB and NZSIS and to provide guidance to the agencies on how certain lawful activities should be carried out.
3. In 2017, prior to the Act coming into force, the Department of the Prime Minister and Cabinet developed the MPSs on behalf of the Minister Responsible for the GCSB and NZSIS.
4. More detailed information about the MPSs, along with a sample MPS are provided at Attachments A and B.

## The ministerial policy statements are required to be reviewed every three years

---

5. Section 214 of the Act states that the MPSs must be reviewed within three years from the date which they are signed. This means that all ministerial policy statements need to be reviewed and reissued before September 2020.

## We propose the following approach for reviewing and reissuing the ministerial policy statements

---

### The approach to reviewing the MPSs

6. When the MPSs were developed on behalf of the previous minister, we took the following approach:
  - *The MPSs should be largely principle-based* – they are intended to provide guidance, not substitute for the operational policies and procedures each agency will have in place to the various activities
  - *The MPSs should be publicly available*

- *MPSs should apply jointly to the NZSIS and GCSB where possible – in order to apply a consistent framework for both agencies*
- *Each MPS should be self-contained and the linkages should be clear*
- *Each MPS will have its own consultation plan – as the agencies with an interest in the MPS review will vary according to the activity the MPS covers.*

7. If you agree, we propose to take the same approach in reviewing the MPSs.

#### **How we will review the MPSs**

8. We will work closely with the policy, legal and operational branches of the NZSIS and GCSB during the review, in accordance with a protocol to be agreed between DPMC and the agencies. Working with the agencies, we will consider the following factors:

- How the MPSs have been incorporated into the operations of the agencies
- Whether they have provided clear and sufficient guidance to the activities the agencies undertake and facilitate the functions of the agencies under the Act
- Whether there have been any impediments to the operationalisation of the MPSs
- If there have been unintended consequences, or other issues, including on the effectiveness and efficiency of the agencies to an unjustified degree
- The comments and views of relevant oversight bodies, including the Inspector-General of Intelligence and Security (IGIS).

9. We will work with the agencies to prioritise the MPSs for review and review them in four tranches. This will allow the work to be spread over time in a manageable way, alongside other priority areas of work.

10. If there is a difference in the interpretation of the Act, or other aspects of the law during the review, Crown Law advice will be sought to provide the definitive Crown view.

#### **The overseas cooperation ministerial policy statement will be reviewed first**

---

11. The recently released report by the IGIS recommended an early review of the overseas cooperation MPS.

12. Section 207 of the Act requires the responsible Minister to issue an MPS to provide guidance to the intelligence and security agencies in relation to these matters:

- Co-operating with an overseas public authority
- Providing advice and assistance to an overseas public authority
- Sharing intelligence with an overseas public authority.

13. The IGIS, in her report *Inquiry into possible New Zealand intelligence and security agencies' engagement with the CIA detention and interrogation programme 2001-2009* (the IGIS report), recommended an early review of the MPS – Cooperation of

New Zealand intelligence and security agencies (GCSB and NZSIS) with overseas public authorities (the overseas cooperation MPS) and made several suggestions to address gaps in the MPS.

14. When the overseas cooperation MPS was developed in 2017 we were aware of the forthcoming IGIS report and included a statement within the MPS that it would be reviewed and reissued when the IGIS Inquiry was completed. In DPMC's response to the IGIS report we agreed to consider the recommendation within the review of the overseas cooperation MPS and to work with the IGIS as the review progressed.

**What will the review of the overseas cooperation ministerial policy statement consider?**

15. The IGIS report states that the MPS should unambiguously set out New Zealand's obligations relating to the law of torture and complicity in torture. This was not able to be achieved when the MPS was developed in 2017. The Ministry of Foreign Affairs and Trade (MFAT) is leading a process to clarify New Zealand's obligation, at international law, not to be complicit in the internationally wrongful acts of foreign partners. The advice MFAT provides as part of that process will be relevant to a range of agencies across government, including the intelligence and security agencies, New Zealand Defence Force, New Zealand Police, Customs, and DPMC. It will be relevant to understanding New Zealand's obligation not to be complicit in torture as well as its obligation not to be complicit in a range of other internationally wrongful acts. This work will inform the review of the MPS.
16. The IGIS report also identified the following gaps in the MPS, which will be considered within the review:
  - the MPS does not state that the prohibition of torture is non-derogable
  - the MPS does not specify the circumstances in which 'tainted' information might be justified
  - it does not reflect that protecting property should not be accorded primacy over protecting human rights
  - the threats or risks that, when identified, would allow the agencies to share information through human rights abuses, lack clarity
  - there is inconsistency in whether 'tainted' information may or should be passed to relevant law enforcement agencies
  - it is unclear what 'unsolicited' means in the context of an intelligence-sharing relationship
  - the MPS refers to situations where intelligence is suspected to have been gained through torture which indicates a 'credible' security risk, which does not reconcile with the statement that information gained by torture is inherently unreliable.
17. The review will consider whether there needs to be consolidated guidance for all agencies working within other states' security systems, to ensure that assistance is consistent with New Zealand's domestic and human rights obligations and consistent across government (in addition to the intelligence and security agencies, this would include all security agencies, including NZ Police, the New Zealand Defence Force, MFAT, Immigration New Zealand and New Zealand Customs).



## The Act requires the minister to consult on the review of the ministerial policy statements

---

18. Section 211 of the Act states that the Minister must consult with IGIS, any other Minister with an interest in the proposed policy statement and any other person that the Minister considers appropriate. When the MPSs were developed, DPMC consulted on the Minister's behalf. Agencies who were consulted included the Office of the Privacy Commission, the Human Rights Commission, Department of Internal Affairs, MFAT, Ministry of Justice, Ministry for Primary Industries, New Zealand Police, New Zealand Customs Service and Ministry of Transport.

### Consultation on the overseas cooperation MPS

19. The IGIS report recommended that 'relevant NGOs' are consulted on the review of the overseas cooperation MPS. While not listed in the report, relevant NGOs in this context might be Amnesty International, Human Rights Watch and the International Committee of the Red Cross.
20. Consultation with NGOs is not a requirement of the Act, and is a decision for the Minister. The IGIS report does not set out the benefits of consulting with relevant NGOs, although we expect it is because these organisations have a specific focus and oversight role in relation to international human rights, and can provide an alternative view that is not solely that of the government.
21. A potential risk of consulting with NGOs is that it may cause difficulties if their views are not reflected in the final MPS for any reason, or if the consulted parties have differing views. Consulting with NGOs is likely to add time to the review process. It may also set expectations that we would consult on each of the MPSs, which would risk the completion of the review and reissue of the MPSs in the required time.
22. As with the development of this MPS, we will consult with the Human Rights Commission in reviewing the overseas cooperation MPS. As the central agency for advocating and promoting human rights in New Zealand our view is that consultation with the Human Rights Commission is sufficient to gather a specific human rights perspective.
23. If you wish to consult with relevant NGOs on the overseas cooperation MPS we are able to do this on your behalf. We can prepare advice on the specific NGOs that might be suitable.

### Consultation

---

24. The NZSIS, the GCSB and MFAT were consulted on this briefing and their views incorporated.

### Next steps

---

25. We are available to discuss the proposed review of the MPSs with you if you wish.
26. If you agree with the recommendations, we will, in collaboration with the agencies, develop a detailed plan for the review, including opportunities to consult with you on the drafts as

they progress. We will provide this plan to your office, for your information.

27. We will update you regularly as the review progresses.

**Proposed timing**

28. The MPSs will be reviewed in tranches. We will set out the timing in the forthcoming detailed plan.

29. The review of the overseas cooperation MPS will begin immediately. Our aim is to provide the draft MPS for your consideration by the end of 2019 (subject to the work MFAT is leading to formalise a statement of New Zealand's obligations regarding the law of torture and complicity in torture).

30. The IGIS report also recommended that the agencies' Joint Policy Statement on Human Rights Risk Management (the JPS) is reviewed. The review of the JPS will need to occur following the review of the overseas cooperation MPS, so that any changes to the MPS are reflected in the JPS.

31. The statutory deadline for completion of the review is September 2020. We will aim to have all MPSs reviewed and reissued by early August 2020.

Attachments:	
Attachment A:	Ministerial policy statements – background information
Attachment B:	Sample ministerial policy statement – Creating and maintaining a legal entity under subpart 2 of Part 3 of the Intelligence and Security Act 2017

## ATTACHMENT A

### Ministerial policy statements – background information

#### What activities do the ministerial policy statements cover?

1. The activities the MPSs cover generally relate to those lawful activities that have a level of risk associated with them, intrusion on privacy, or involve some kind of deception. The Act requires the Minister to issue MPSs on these activities:
  - Providing information assurance and cybersecurity activities with the consent of the party to whom those services are provided
  - Acquiring, using and maintaining an assumed identity
  - Creating and maintaining a legal entity (such as a cover company)
  - Collecting information lawfully from persons without an intelligence warrant or authorisation given under section 78 (human intelligence activities)
  - Conducting surveillance in a public place
  - Obtaining and using publicly available information (open source information)
  - Making requests for information from other agencies under section 121 of the Act
  - Information management
  - Making false or misleading representations about being employed by an intelligence and security agency under section 228
  - Activities covered by the exemption from the Land Transport (Road User) Rule 2004 that is conferred by section 231 of the Act
  - Cooperation with overseas public authorities, including providing advice and assistance to and sharing intelligence with overseas public authorities.
2. The Minister may also issue additional MPSs where he or she considers that guidance on any activity is desirable.
3. The MPSs are publicly available on the New Zealand Intelligence Community website.

#### What effect do the ministerial policy statements have?

4. The Directors-General and all employees of GCSB and NZSIS must consider the requirements and guidance in an MPS when carrying out the activity covered by it. While it is not compulsory for an employee to comply with a ministerial policy statement, there would need to be a very good reason for not complying and the employee would need to be able to justify that.
5. The MPSs require GCSB and NZSIS to put policies and procedures in place to ensure employees are acting lawfully and appropriately when carrying out the activities to which the ministerial policy statements relate. They also require GCSB and NZSIS to consult other agencies with an interest or expertise in matters related to the activity being carried

out. Some MPSs also set out particular training that must be provided to employees who are carrying out the activity to which the particular MPS relates.

6. The Inspector-General of Intelligence and Security must also take any MPS into account when conducting an inquiry into the activities of the intelligence and security agencies.

**What information do the ministerial policy statements contain?**

7. As required by section 210 of the Act, the MPSs contain guidance on:
  - Procedures for authorising individual employees to carry out the activity (if applicable)
  - Any protections that must be in place in relation to the activity
  - Any restrictions on the activity that must be applied.

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

## ATTACHMENT B

Ministerial Policy Statement example – 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



# Briefing

## REVIEW OF THE OVERSEAS COOPERATION MINISTERIAL POLICY STATEMENT: PROPOSED CONSULTATION PLAN

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

Date	24/01/2020	Priority	Routine
Deadline	31/01/2020	Briefing Number	1920NSP/031

### Purpose

This briefing:

- Seeks your agreement to a consultation plan for consulting with non-government organisations on the Ministerial Policy Statement: *Cooperation of New Zealand intelligence and security agencies (GCSB and NZSIS) with overseas public authorities.*
- Updates you on the review of the Ministerial Policy Statements.

### Recommendations

1. **Note** that in September 2019 you agreed the Department of the Prime Minister and Cabinet would consult, on your behalf, with non-government organisations on the review of the overseas cooperation ministerial policy statement
2. **Agree** that the Department of the Prime Minister and Cabinet consult with the following organisations:
  - 2.1 Human Rights Foundation YES / NO
  - 2.2 New Zealand Council for Civil Liberties YES / NO
  - 2.3 Amnesty International YES / NO
  - 2.4 Privacy International YES / NO
3. **Agree** to the attached consultation plan YES / NO

REVIEW OF THE OVERSEAS COOPERATION MINISTERIAL POLICY STATEMENT:  
PROPOSED CONSULTATION PLAN

1920NSP/031

4. **Note** that we aim to deliver the first two draft Ministerial Policy Statements to consider for Ministerial consultation in early February 2020.

  
Tony Lynch  
**Deputy Chief Executive  
National Security Group**

23 / 01 / 2020  
...../...../.....

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

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

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

Contact for telephone discussion if required:

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



# REVIEW OF THE OVERSEAS COOPERATION MINISTERIAL POLICY STATEMENT: PROPOSED CONSULTATION PLAN

## Purpose

---

This briefing:

- Seeks your agreement to a consultation plan for consulting with non-government organisations on the Ministerial Policy Statement (MPS): *Cooperation of New Zealand intelligence and security agencies (GCSB and NZSIS) with overseas public authorities* (the Overseas Cooperation MPS).
- Updates you on the review of the MPSs.

## You agreed to consult with NGOs on the Overseas Cooperation MPS

---

1. In September 2019, we briefed you (1920NSP/010) on the proposed approach to reviewing the MPSs required under Section 207 of the Intelligence and Security Act 2017 (the Act). We noted that the review of the Overseas Cooperation MPS would be started first.

### The Overseas Cooperation MPS

2. Section 207 of the Act requires the responsible Minister to issue guidance to the intelligence and security agencies on:
  - Co-operating with an overseas public authority
  - Providing advice and assistance to an overseas public authority
  - Sharing intelligence with an overseas public authority.
3. The first Overseas Cooperation MPS was issued in 2017 (Attachment A). The MPS provides guidance for the GCSB and NZSIS in relation to all forms of cooperation with overseas public authorities. It states that, when making decisions related to foreign cooperation, the agencies must have regard to the principles of legality, human rights obligations, necessity, reasonableness and proportionality, protections for New Zealanders, information management, and oversight. It also sets out the procedures to authorise intelligence cooperation, assistance and sharing, and the protections and restrictions that need apply.

### The IGIS report recommended early review of the Overseas Cooperation MPS

4. At the time of issue of the MPS, the Inspector General of Intelligence and Security (IGIS) was inquiring into whether NZSIS and GCSB had any connection to the CIA's enhanced interrogation, detention and rendition programme in Afghanistan between 2001-2009 (the IGIS Report). The Overseas Cooperation MPS noted this work by the IGIS was ongoing, and that 'when completed, the conclusions from that Inquiry may give cause for the issuing Minister to review and reissue the MPS'.

5. The IGIS report recommended an early review of the Overseas Cooperation MPS, having regard to the gaps that were identified in the report. It also recommended consulting with relevant NGOs on the review of the MPS, which you subsequently agreed to.

## **Consultation will improve the support and quality of the Overseas Cooperation MPS**

---

6. The Overseas Cooperation MPS has strong public interest elements. This MPS requires significant human rights responsibilities and implications (particularly relating to torture) be considered by intelligence agencies when cooperating with overseas authorities. Conducting engagement that considers the concerns and expertise of relevant NGOs will strengthen the Overseas Cooperation MPS and potentially increase confidence in the intelligence agencies.
7. To refine the scope of consultation, officials have considered the recommendations in the IGIS Report alongside the recent consultation on the United Kingdom's *Consolidated Guidance to Intelligence Officers and Service Personnel on the Detention and Interviewing of Detainees Overseas, and on the Passing and Receipt of Intelligence Relating to Detainees*. We propose the following key areas of focus for consultation:
  - How to clearly articulate the responsibilities and obligations relating to torture within the MPS (including the non-derogable nature of torture).
  - Defining exceptional circumstances, public emergencies and/or credible risks to national security where 'tainted' information, i.e. information likely obtained by torture, might be passed to relevant law enforcement agencies.
  - How agencies should weigh up competing rights and interests, such as loss of life, significant personal injury, critical national infrastructure, and/or property.

## **We recommend early targeted consultation with a small number of relevant organisations**

---

8. We recommend undertaking a targeted consultation with a small number of NGOs that promote and defend human rights, and understand New Zealand's international human rights obligations. The organisations we suggest consulting are:
  - Human Rights Foundation
  - New Zealand Council for Civil Liberties
  - Amnesty International
  - Privacy International.
9. These organisations have been suggested as they have been nominated by the IGIS as leaders domestically and/or internationally within the human rights NGO community, they have strong engagement records on policy, and they have a New Zealand based contact point that can be used to engage their wider organisation and/or network. Other NGOs considered included Transparency International New Zealand and the Privacy Foundation New Zealand. We have limited the number to the selected NGOs to enable the best use of limited consultation resource and to avoid duplication.

10. The draft proposed consultation document (Attachment B) contains further details, including consultation questions based on the suggested focus areas. We propose to send the agencies the consultation document and seek written feedback.
11. Responses from this consultation will be balanced alongside other consultation required under the Act. The Act requires you to consult with the Inspector-General of Intelligence and Security, any other Minister with an interest in the policy statement and any other person that you consider appropriate. In addition to the GCSB and the NZSIS, consultation amongst Government agencies may include MFAT, MOJ, NZDF, CLO, the Privacy Commissioner, and the Human Rights Commission.
12. We are also engaging with MFAT's ongoing development of legal advice to agencies regarding aid and assistance at international law, to ensure the MPS is aligned with this advice.

### **There are risks with consulting with non-government organisations**

13. We have identified the following risks and mitigations as part of the consultation plan.

Risk	Mitigation
Participants feel their views are not taken into consideration and criticise the review	DPMC will respond and engage with participants to ensure clarity and transparency where possible
Participants are unable to contribute their written submission within the timeframe available	DPMC will discuss individual circumstances as they may arise, and accept verbal submissions if necessary
There is negative public or media interest in the review	DPMC will work with your office, the NZSIS and GCSB to develop reactive talking points to respond to media interest
Participants wish to contribute to other MPS reviews, or international cooperation procedures or matters beyond the scope of this MPS	The consultation document will make it clear that we are only seeking input into the review of this MPS, given the significant interest in human rights issues. The consultation document will also make it clear that we are not seeking feedback on operational matters relating to cooperating with foreign authorities.

### **Next Steps**

14. If you agree to the proposed consultation plan, we will contact the proposed NGOs in February 2020.
15. We are reviewing the 11 MPSs in four tranches and have begun the first tranche. Aside from the Overseas Cooperation MPS, the first tranche includes the MPSs on *Road user rules exemption* and *Conducting surveillance in a public place*. We expect to have a draft

of these MPSs for consultation with your ministerial colleagues by early February 2020.

- 16. We remain available to discuss with you, or your office, the review of the MPSs if you wish.

### Consultation

---

- 17. The Office of the IGIS was consulted on the proposed list of NGOs for consultation. The GCSB and NZSIS were consulted on this briefing and their views incorporated.

Attachments:		
Attachment A	Unclassified	Current Overseas Cooperation MPS
Attachment B	Unclassified	Draft Overseas Cooperation MPS NGO Consultation Document

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

# Attachment A

---

## Current Overseas Cooperation MPS

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982



## *Ministerial Policy Statement*

# Cooperation of New Zealand intelligence and security agencies (GCSB and NZSIS) with overseas public authorities

### **Summary**

It is important for New Zealand's security for the Government Communications Security Bureau (GCSB) and New Zealand Security Intelligence Service (NZSIS) to cooperate with overseas public authorities, including overseas intelligence agencies.

This ministerial policy statement (MPS) provides guidance for GCSB and NZSIS in relation to all forms of cooperation with overseas public authorities. In making decisions related to foreign cooperation, employees must have regard to the following principles: legality, human rights obligations, necessity, reasonableness and proportionality, protections for New Zealanders, information management and oversight. This MPS also specifies certain additional matters to be included in internal policy and procedures.

### **Definitions**

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

**Cooperation** means any form of interaction, whether reciprocal or not, with an overseas public authority, including but not limited to training, advice, assistance, and sharing of information, intelligence, analysis, methods and technology.

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

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

**Overseas public authority** means a foreign person or body that performs or exercises any public function, duty, or power conferred on that person or body by or under law.

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

## Purpose

1. This MPS is issued by the Minister Responsible for the GCSB and the Minister in Charge of the NZSIS pursuant to section 207(1) of the Act.
2. The purpose of the MPS is to provide guidance to GCSB and NZSIS on the conduct of activities that involve cooperation with overseas public authorities. 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 her 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). A copy of this MPS will also be provided to the Intelligence and Security Committee of Parliament.
4. Every employee making decisions or taking any action related to cooperating with an overseas public authority 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 cooperating with an overseas public authority, which includes providing advice and assistance to an overseas public authority and sharing intelligence with an overseas public authority. These activities may occur in relation to any of the functions of GCSB and NZSIS as specified or allowed for in sections 10 to 15 of the Act.
6. For the purposes of this MPS a broad interpretation of cooperation applies, in that specific activities may or may not be reciprocal, but will in some way involve GCSB or NZSIS interaction with an overseas public authority (also referred to as a foreign partner). To this end, it includes the provision of services, advice, assistance and intelligence which is not reciprocated, as well as reciprocally sharing intelligence, acting cooperatively on a project, or providing and receiving services, advice, and assistance. Cooperation may include an overall cooperative relationship between GCSB or NZSIS and an overseas public authority, interactions between employees of GCSB or NZSIS and the overseas public authority, or specific activities that occur as part of cooperation with a foreign partner.
7. GCSB and NZSIS may only request overseas public authorities to carry out activities that, if carried out by GCSB or NZSIS without an authorisation would be unlawful, in accordance with an authorisation issued under part 4 of the Act. In addition, the Directors-General of GCSB and NZSIS may request those authorities (or their personnel) to assist GCSB or NZSIS with giving effect to an authorisation (see section 51(1)). The carrying out of these types of authorised activities must be conducted consistently with the Act and the terms of the relevant authorisation, including any restrictions or conditions set out in the authorisation. This MPS does not apply to requests for assistance and activities which are carried out under an authorisation issued under part 4 of the Act.
8. The primary purpose of this MPS is to provide guidance on determining which overseas public authorities GCSB and NZSIS should engage with, and how that engagement should be

regulated, including guidance on the types of activities that are appropriate to undertake with those parties. To the extent that it arises through cooperation with an overseas public authority, the MPS also addresses issues associated with the operational use of intelligence gained from a foreign partner.

## 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;
  - b) The provision of protective security services, advice and assistance;
  - c) Cooperation with other public authorities to facilitate their functions; and
  - d) Cooperation with other entities to respond to imminent threat.
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.

### *New Zealand's intelligence and security relationships*

12. The mandate provided by the agencies' objectives and functions is a New Zealand-centric one. Foreign cooperation is based on furthering New Zealand's interests and fulfilling any international obligations New Zealand has.
13. GCSB and NZSIS may cooperate with overseas public authorities in fulfilling any of GCSB's and NZSIS's functions. New Zealand gains significant value from international intelligence sharing and cooperation arrangements, particularly within the current climate of global and transnational threats. Through foreign intelligence partnerships and other cooperation, GCSB and NZSIS are able to draw on a much greater pool of information, skills and technology than would otherwise be available to them. Close and reliable relationships with overseas public authorities help GCSB and NZSIS to prioritise and focus their limited resources on the areas most important to New Zealand, while having access to resources that would not normally be available.
14. For example, a foreign partner may have access to information that requires specific linguistic, ethnic or cultural backgrounds to collect and analyse which New Zealand does not possess. As part of their intelligence collection and analysis function, GCSB and NZSIS may seek to obtain that intelligence. Similarly, GCSB or NZSIS might provide intelligence to an overseas public authority so that authority can take action to address a threat to New Zealand's national security (such as a threat to New Zealanders overseas), or to contribute to New Zealand's international relations with the partner country.
15. In the context of protective security services, advice and assistance, GCSB or NZSIS might provide technology or expertise to an overseas public authority (which might include seconding staff) to support that authority with its own protective security requirements, such as systems for vetting security cleared personnel, or detecting cybersecurity threats. This



- advice and assistance could contribute to New Zealand's national security by mitigating common threats and developing international relations with the partner countries, and contribute to New Zealand's economic well-being by reducing risks to New Zealand companies operating overseas.
16. The closest relationships that GCSB and NZSIS have with overseas public authorities are those with equivalent agencies from Australia, Canada, the United Kingdom and the United States (often referred to as the "Five Eyes" partners). The relationships between Five Eyes partners are long-running, reciprocal, cover a wide range of topics, and involve a high degree of mutual trust, honesty and respect. The relationships provide New Zealand with knowledge and capability far beyond what we can afford on our own.
  17. These relationships work effectively due to the shared values and histories of the five countries and the strong relations between the governments of those countries in general. The depth of the Five Eyes relationship means that disparities in size, power and influence do not prevent any member from acting in the best interests of their own government, and members expect to be able to disagree on specific matters without damaging the broader relationship.
  18. GCSB and NZSIS may also cooperate with overseas public authorities from other countries. This cooperation may occur on a routine or relatively ad hoc basis. The reasons for cooperating with such authorities may vary widely and may occur in the course of performing any of the agencies' functions and as part of contributing to any of their objectives. It is essential to New Zealand's ability to protect its national security, international relations and economic well-being to share information and intelligence with agencies outside traditional partnerships.

#### *International obligations*

19. New Zealand may be subject to international obligations to cooperate with overseas partners, in order to promote the exchange of information to help improve international responses to threats to global peace and security. For example, United Nations Security Council Resolution 1373 (2001) calls on states to "find ways of intensifying and accelerating the exchange of operational information, especially regarding actions and movements of terrorist persons or networks". Under this resolution, Member States are required to have in place procedures and mechanisms that encourage exchange of information in accordance with international and domestic law, which includes international human rights obligations.
20. The many positive benefits of New Zealand's participation in foreign intelligence and security relationships do not override the rights of New Zealanders and the international human rights obligations New Zealand has adopted through their incorporation into domestic law. New Zealand is also subject to other international obligations, including through customary international law and as a member of the United Nations. For example, New Zealand is bound by United National Security Council Resolution 1456 (2003), which requires Member states to "ensure that any measure taken to combat terrorism comply with all their obligations under international law, and should adopt such measures in accordance with international law, in particular international human rights, refugee and humanitarian law".
21. New Zealand's core international human rights obligations, including those at customary international law, are detailed at Appendix One. They include the right to life, the right not to be subjected to torture, the right not to be subjected to cruel, inhuman or degrading treatment or punishment, and the right to liberty and security of the person.

22. The New Zealand Government has a long-standing and strong opposition to the use of torture, cruel, inhuman or degrading treatment or punishment (including the death penalty) in all cases and under all circumstances, including in response to threats to national security. New Zealand is committed to actively preventing torture, cruel, inhuman or degrading treatment or punishment, and will not, by act or omission, encourage, aid, or abet such action.

*Duty to act with due diligence*

23. Section 17(a) of the Act imposes a general duty on GCSB and NZSIS to act in accordance with New Zealand law and all human rights obligations recognised by New Zealand law. Sections 10(3) and 12(7) also explicitly impose an obligation on the responsible Minister to be satisfied the agencies will be acting consistently with such law when authorising the sharing of intelligence, analysis and threat reporting with foreign partners. Compliance with this obligation necessitates a practice of due diligence by the Directors-General of GCSB and NZSIS in relation to cooperation with overseas public authorities. The guidance in this MPS provides a framework for exercising that due diligence when determining whether it will be appropriate to engage with a particular overseas public authority, and when determining that the proposed activities are consistent with the law – particularly with respect to ensuring that GCSB and NZSIS do not become complicit in human rights abuses.
24. The Directors-General have a duty to take steps as are reasonable in the circumstances of each particular situation to identify risks of human rights being breached by partner countries and international actors. To ensure that agencies are not associated (either directly or indirectly) with activities that may be unlawful or improper, as a result of cooperation with an overseas public authority, it is expected that GCSB and NZSIS will establish an awareness of and regularly monitor the human rights practices of any overseas public authorities with which the agencies cooperate. The agencies are also expected to further enquire when there is an indication that human rights breaches might occur in a situation, and decline or stop cooperating with the overseas public authority where a real or substantial risk of breach of human rights obligations (such as the prohibition of torture) is identified.
25. Failure to act in accordance with the provisions of the Act and this MPS could lead to possible criminal responsibility for employees of GCSB and NZSIS. For example, Section 3 of the Crimes of Torture Act 1989, which applies to activities conducted within or outside New Zealand, makes it a crime for a public official or anyone acting in an official capacity to attempt or to commit an act of torture, to act or omit to act in a way that aids any person to commit an act of torture, to abet any person in the commission of an act of torture, or to incite, counsel, procure or conspire with any person to commit an act of torture, and to be an accessory after the fact to an act of torture.

*Unsolicited intelligence*

26. The absolute prohibition in international law (and which is incorporated in New Zealand law) on the use of information gained through torture for evidentiary purposes arises from the need to remove any incentives to torture and recognises that such information is inherently unreliable. This obligation is non-derogable – it cannot be violated by states under any circumstances.

27. There may be exceptional circumstances where unsolicited intelligence is received by GCSB or NZSIS that indicates a credible national security threat to New Zealand or risk to New Zealanders that has been, or is suspected to have been, obtained through human rights abuses committed by another party.
28. GCSB and NZSIS do not have an enforcement function in relation to measures to protect national security. If intelligence is received that indicates a credible risk to the safety of New Zealanders that requires action to be taken to protect lives and property, GCSB and NZSIS must provide that information to the relevant enforcement agency. The information will not be used for evidentiary purposes in legal proceedings.

### **Principles**

29. The following principles constitute a framework for good decision-making and must be taken into account by GCSB and NZSIS when cooperating with overseas public authorities in the performance of one or more of the agencies' functions. All forms of cooperation with overseas public authorities, at all levels, should be subject to ongoing review as to whether it continues to be consistent with these principles.

### *Legality*

30. GCSB and NZSIS must ensure that cooperation with overseas public authorities is conducted in accordance with New Zealand law and all human rights obligations recognised by New Zealand law. GCSB and NZSIS should also have regard to New Zealand's human rights obligations at international law, including customary international law (see Appendix One).
31. For all forms of cooperation with overseas public authorities, GCSB and NZSIS must have internal policies in place that ensure the agencies act in accordance with New Zealand law and all human rights obligations recognised by New Zealand law; and must have procedures in place to ensure those policies have been adhered to. Where appropriate, legal advice should be sought.
32. Where Ministerial approval for cooperation is required, GCSB and NZSIS have a positive obligation to provide sufficient information regarding the legality of cooperation with overseas public authorities to the Minister, in order for the Minister to determine whether the requirements under sections 10(3) and 12(7) of the Act are met.
33. Where there may be uncertainty or cause for concern as to whether cooperation with an overseas public authority is lawful, specific information detailing the nature of the cooperation and the factors that gave rise to that uncertainty or concern (such as examples of previous actions by the foreign partner, external reports, or advice from the Ministry of Foreign Affairs and Trade) should be provided to the responsible Minister (in the case of Ministerial approvals) to assist decision-making, or to the Director-General (in the case of internal approvals).
34. Where necessary, the Ministry of Justice should be consulted on New Zealand's human rights law and information sought from the Ministry of Foreign Affairs and Trade regarding New Zealand's international human rights obligations and the adherence of other countries to these obligations.

### *Human rights obligations*

35. GCSB and NZSIS must not undertake any activity in cooperation with an overseas public authority, including receiving or sharing any intelligence, where GCSB or NZSIS knows or assesses that there is a real risk that the activity will lead to or has been obtained as a result of human rights breaches in any country, against any person(s). In these circumstances, the continued receipt or sharing of intelligence should cease, subject to a reassessment in accordance with legal obligations, the principles in this MPS and relevant policies.
36. This provides a duty to apply due diligence: GCSB and NZSIS are to assess the likelihood of human rights breaches occurring (or having occurred) in connection with any sharing of intelligence or cooperation by the agencies with an overseas public authority, including in any subsequent actions taken by that public authority as a result of the cooperation or sharing of intelligence.
37. To avoid any complicity in human rights breaches by an overseas public authority, when assessing this likelihood, GCSB and NZSIS must take into account factors such as:
  - 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;
  - whether the country has ratified relevant international human rights treaties, including any reservations that may have been made;
  - whether the country has mechanisms for independently investigating breaches of human rights;
  - whether the country has an independent judiciary with jurisdiction to hear cases relating to breaches of human rights;
  - whether the country has an established history of compliance with human rights obligations;
  - whether the country has an established history of investigating and prosecuting human rights breaches; and
  - 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.
38. When authorising the provision of intelligence and analysis, or the provision of threat reports produced from the provision of information assurance and cybersecurity activities, to an overseas public authority, the responsible Minister must be satisfied that GCSB and NZSIS will be acting in accordance with New Zealand domestic law, including all human rights obligations recognised by New Zealand law.
39. The Minister must be satisfied of this on the basis of information provided to him or her by GCSB or NZSIS about the particular proposal to share intelligence, analysis or threat reporting. The Minister's authorisation may be made on a case-by-case basis or may take the form of a broader standing authorisation, for example to share specific categories of intelligence, analysis or threat reporting with certain overseas public authorities, or to share the full range of intelligence, analysis or threat reporting within an established intelligence and security relationship with a foreign country, groups of countries or overseas public authority.

40. A request to share intelligence, analysis and threat reporting with a foreign partner, whether on a case-by-case basis, or within the context of a broader standing authorisation, must include information about the specific proposal and must include an assessment of the human rights practices of the foreign partner, or describe the process by which the agencies will make that assessment. The assessment must be based on:
- the human rights record of the country (as reflected in the considerations at paragraph 37 above)
  - any particular risks to human rights associated with the proposed cooperation and how likely it is that breaches could occur; and
  - factors that mitigate the likelihood of human rights breaches occurring. Such factors might include the existence and effectiveness of mechanisms for monitoring or reviewing compliance with human rights obligations, 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 how likely the foreign partner is to comply with caveats associated with cooperation or use of information.
41. The decision to authorise the sharing of intelligence, analysis or threat reporting with a foreign partner, whether made by the Minister on a case-by-case basis or by the agencies within a broader standing authorisation, must also consider:
- all applicable legal obligations under New Zealand and international law, and any relevant international commitments New Zealand may have; and
  - the purpose of the intelligence sharing, including how it contributes to GCSB's and NZSIS's statutory objectives to contribute to the protection of New Zealand's national security, the international relations and well-being of New Zealand, and the economic well-being of New Zealand.
42. The responsible Minister may issue standing authorisations for GCSB or NZSIS to share specific classes of intelligence, analysis and threat reporting with certain overseas public authorities, or to share intelligence, analysis and threat reporting with a specific overseas public authority or with a particular country or group of countries. When issuing a standing authorisation, the Minister must be satisfied on the basis of an assessment which considers the same factors in paragraphs 40 and 41 above. Standing authorisations may specify conditions, limits or exclusions that apply in respect of the sharing of intelligence, analysis and threat reporting under the authorisation. The Minister will specify thresholds of risk at which decisions made under a standing authorisation must be referred back to the responsible Minister.
43. The existence of a standing authorisation does not excuse GCSB and NZSIS of the obligation to undertake ongoing monitoring to ensure that cooperation undertaken under the authorisation remains consistent with the framework in this MPS. In particular, the agencies must conduct a risk assessment of human rights breaches occurring if there is any reason to believe a specific instance of cooperation might lead to such an infringement. Further, if there is evidence that a human rights breach has occurred, or there are changes to domestic policy or practice in any country subject to a standing authorisation that may increase the likelihood of violations of human rights, the standing authorisation must be reviewed by the responsible Minister.

44. Where Ministerial authorisation for cooperation is not required, GCSB and NZSIS must have processes that require internal authorisation to cooperate with an overseas public authority to be granted by appropriately senior staff, according to an assessment of the risk of human rights breaches connected with that cooperation. Where there is a reasonable basis for concern about a country's human rights record or that the cooperation in question might involve complicity in breaches of human rights, GCSB and NZSIS must seek authorisation from the responsible Minister before undertaking any cooperation. GCSB and NZSIS must provide the Minister with an assessment that addresses the factors outlined at paragraphs 40 and 41.
45. If GCSB or NZSIS become aware that their cooperation with an overseas public authority means GCSB or NZSIS may have been complicit in human rights breaches the agency must immediately suspend cooperation with that authority (and any others related to it) and notify the responsible Minister and the Inspector-General of Intelligence and Security, and if necessary, the Solicitor-General. An internal review to determine whether agency policies and procedures were correctly applied in respect of the cooperation must also be conducted by the relevant agency.
46. In the event GCSB or NZSIS receives unsolicited information indicating a credible national security risk to New Zealand or risk to the safety of New Zealanders, but that has been, or is suspected to have been, obtained through human rights abuses committed by another party the Directors-General will consider the need to ensure public safety and the protection of life and property in determining whether to pass that information to the relevant enforcement agency. In considering whether to pass on the information for operational purposes, GCSB and NZSIS must be mindful that the reliability of such information may be limited. Where information of this nature is passed on, the responsible Minister and the Inspector-General of Intelligence and Security must be informed as soon as practicable.

#### *Necessity*

47. Cooperation by GCSB or NZSIS with any foreign partner must be for the purpose of protecting New Zealand's national security, the international relations and well-being of New Zealand, and the economic well-being of New Zealand. Specific cooperation with overseas public authorities should only occur for purposes necessary to support the agencies to perform their statutory functions. This may include building the capacity of GCSB or NZSIS to perform a particular statutory function, or for establishing or maintaining an international relationship that will support GCSB or NZSIS to perform their statutory functions.

#### *Reasonableness and proportionality*

48. The impact of 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.
49. Relevant factors in determining the reasonableness and proportionality of cooperation with an overseas public authority include:
- having a clear understanding of the nature and purpose of the specific activities and any subsequent actions that are likely to result;

- having a clear understanding of the nature and purpose of the intelligence and security relationship with the particular overseas public authority;
  - being aware of the status of the bilateral relationship with the country as a whole (especially any issues or areas of sensitivity between New Zealand and the partner country that could have a bearing on the proposed activities);
  - any limitations or restrictions on activity that either party has; and
  - any protections that may be in place in relation to the activity or to intelligence provided or received.
50. For example, when New Zealand is seeking assistance or intelligence or information from partners, GCSB or NZSIS should be clear as to why they seek the assistance or intelligence or information from the partner country, and about the expectations of the New Zealand Government that no human rights breaches occur in the provision of that assistance or in the collection or provision of the intelligence or information.
51. Where New Zealand is asked to provide assistance, intelligence or information by overseas partners, GCSB or NZSIS should be as informed as is possible about the particular situation. This should include being aware of the purpose and value of the proposed activity and that there is sufficient evidence, not based on human rights breaches, of the need for the activity.
52. For example, when sharing intelligence, this would include consideration of whether this was reciprocal sharing of intelligence on a routine and systematic basis, as part of a wider intelligence relationship; regular sharing of intelligence but on a case-by-case basis; responding to one-off ad hoc (and potentially urgent) requests for intelligence; or pro-active ad hoc sharing by the agencies to mitigate a risk to a third country.

#### *Protections for New Zealanders*

53. When cooperating with overseas public authorities, GCSB and NZSIS must continue to apply the same protections for New Zealand citizens and permanent residents 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.
54. Where cooperation with an overseas public authority involves the sharing of intelligence or personal information relating to New Zealanders, GCSB and NZSIS must have particular regard to the privacy interests of the New Zealanders when determining whether to disclose that personal information to overseas partners, or when requesting such information from overseas partners. This includes adherence to the [information privacy principles](#) contained in Part 2 of the Privacy Act 1993 as they apply to GCSB and NZSIS. GCSB and NZSIS must be satisfied that the overseas public authority has adequate protections in place for the use and storage of New Zealanders' information, including adequate protections against further sharing with third parties without express consent from GCSB or NZSIS.

#### *Information management*

55. GCSB and NZSIS will take steps to ensure that information obtained by GCSB and NZSIS and subsequently shared with overseas public authorities is managed in accordance with all information management requirements, standards and guidelines that relate to that information (such as the New Zealand Protective Security Requirements, New Zealand

- Government Security Classification System, and New Zealand Information Security Manual), and any other obligations as addressed in the MPS on *Management of information obtained by GCSB and NZSIS*.
56. GCSB and NZSIS are to specify the protection, storage and use (including restrictions on the passing on of that information to any third parties) requirements that are to be adhered to in respect of any information, including personal information about New Zealanders, shared with an overseas public authority. Those requirements will be consistent with the principles in this MPS and the MPS on *Management of information obtained by GCSB and NZSIS*. It is recognised that the overseas public authority may be required to adhere its own national requirements when managing received information and this may conflict with conditions imposed by GCSB or NZSIS. GCSB and NZSIS should seek to be consulted regarding any national requirements of an overseas partner that may lead to shared information being used in a manner that conflicts with restrictions that would apply in New Zealand.

#### *Oversight*

57. GCSB and NZSIS must carry out all cooperation with overseas public authorities in a manner that facilitates effective accountability, transparency and oversight. This includes the use of clear authorisation procedures, the keeping of appropriate records, maintaining up-to-date internal policies and procedures and guidance for staff, and reporting to the responsible Minister on the nature and outcomes of cooperation with overseas public authorities. 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**

58. 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. Those policies and procedures must also address the following additional matters:

##### **Human rights policy**

GCSB and NZSIS must have a policy setting out the factors that must be considered when assessing whether a real risk of human rights breaches may exist in connection with cooperation with overseas public authorities. This policy must also include what specific information is required to be provided to the responsible Minister before authorisation (either on a case-by-case basis or in the form of a broader standing authorisation) is given to share intelligence or analysis to an overseas public authority.

This policy is important to ensure that employees do not inadvertently place themselves or the New Zealand Government at legal risk by their action or inaction.

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

Foreign policy objectives should be considered in the development and framing of cooperation arrangements with foreign partners. The Ministry of Foreign Affairs and Trade is to be consulted on any proposal to enter into an arrangement with a foreign jurisdiction or international organisation.

GCSB and NZSIS should also seek information from, and have regard to any information provided by, the Ministry of Foreign Affairs and Trade on the status of the bilateral



relationship with a country, and when weighing up factors related to a country's ratification of international human rights treaties and the human rights record of a particular country.

#### **Written basis for new formal arrangements**

All new bilateral or multilateral arrangements relating to cooperation and intelligence sharing with a foreign jurisdiction or overseas public authority must be referred to the Intelligence and Security Committee of Parliament for noting. Such arrangements should be recorded in writing.

GCSB and NZSIS must formulate standard terms for ad hoc cooperation and intelligence sharing, which are to be recorded in an internal policy. These terms are to establish consistent principles, standards and practices that will be applied to ad hoc cooperation and intelligence sharing activities to ensure that GCSB and NZSIS complies with New Zealand law and all human rights obligations recognised by New Zealand law. Those terms should be consistent with this MPS. These terms must be forwarded in draft to the Inspector-General of Intelligence and Security for comment and the final version referred to the Intelligence and Security Committee of Parliament for noting.

#### **Training**

All employees of GCSB and NZSIS must be provided training on all relevant law, policies and procedures in relation to the agencies' human rights obligations. This training should be provided for all existing employees and for new employees at induction, and whenever there are changes or updates to the policies and procedures, to ensure that at all times employees are aware of their obligations.

#### **Compliance with 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.

#### **Health and safety**

All cooperation with overseas public authorities must be undertaken consistently with GCSB's and NZSIS's obligations under the Health and Safety at Work Act 2015.

### **Authorisation procedures**

59. Within the context of this MPS, the responsible Minister must authorise the following:
  - The provision of any intelligence collected and any analysis of that intelligence to an overseas public authority
  - The provision of threat reports produced as a result of information assurance and cybersecurity activities to an overseas public authority
60. In determining whether to authorise the sharing of intelligence, analysis and threat reporting to an overseas public authority, the Minister must be satisfied that GCSB and NZSIS will be acting in accordance with New Zealand law including all human rights obligations recognised by New Zealand law.
61. The Minister will authorise the sharing of intelligence, analysis or threat reporting with a foreign partner on the basis of information provided to him or her by GCSB and NZSIS. This authorisation may be on a case-by-case basis or in the form of a broader standing authorisation. All requests for authorisation to share intelligence, analysis and threat reporting must include an assessment that addresses all factors listed in paragraphs 40 and 41 of this MPS, or describe how the agencies will make that assessment.

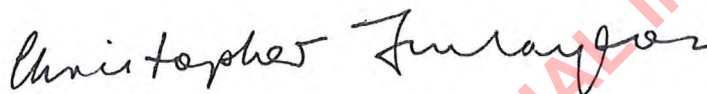
62. GCSB and NZSIS may seek a standing authorisation from the Minister that covers the sharing of specific classes of intelligence, analysis and threat reporting with certain overseas public authorities, or to share intelligence, analysis and threat reporting with a specific overseas public authority or with a particular country or group of countries. A request for a standing authorisation must include an assessment which considers the factors outlined in paragraphs 40 and 41 of this MPS, or describe how the agencies will make that assessment.
63. The Minister may specify conditions, limits or exclusions that are to apply in respect of the sharing of intelligence, analysis and threat reporting with an overseas public authority or country under a standing authorisation. The Minister will specify thresholds of risk at which decisions made under a standing authorisation must be referred back to the Minister. Standing authorisations must be reviewed when this MPS is amended, revoked or replaced, and if a human rights breach occurs or there are changes to domestic policy or practice in the country that may increase the likelihood of violations of human rights.
64. Where Ministerial authorisation for cooperation is not required, there must be clear levels of decision-making for each type of activity that may involve foreign cooperation, which must be documented. GCSB and NZSIS must have in place approval levels that are proportionate to the operational, reputational, legal and health and safety risks in cooperation with overseas public authorities: the greater the risk, the more senior the level of approval required. An assessment of the risk of human rights breaches connected with the foreign cooperation must be carried out, that includes the considerations outlined at paragraphs 40 and 41 of this MPS. Approval levels will include seeking authorisation from the Minister at agreed levels of risk, in particular where there is a reasonable basis for concern about a country's human rights record or that the cooperation in question might involve complicity in breaches of human rights.
65. The Directors-General of GCSB and NZSIS may authorise the passing of unsolicited intelligence indicating a credible national security risk to New Zealand or risk to the safety of New Zealanders that has been, or is suspected to have been, obtained through human right abuses committed by another party, to an enforcement agency. The Directors-General must consider the need to ensure public safety and the protection of life and property, and must be mindful that the reliability of such information is likely to be limited. If such information is passed on to an enforcement agency the responsible Minister and Inspector-General of Intelligence and Security must be informed as soon as practicable.

### Duration of ministerial policy statement

66. This MPS will take effect from 28 September 2017 for a period of three years. The Minister who issued an MPS may, at any time, amend, revoke or replace the MPS.
67. At the time of issue of this MPS, the Inspector-General of Intelligence and Security is undertaking an Inquiry into possible New Zealand engagement with Central Intelligence Agency (CIA) detention and interrogation, 2001-2009, and current intelligence cooperation safeguards. When completed, the conclusions from that inquiry may give cause for the issuing Minister to review and reissue this MPS.

---

Ministerial Policy Statement issued by:



Hon Christopher Finlayson  
Minister responsible for the Government Communications Security Service  
Minister in charge of the New Zealand Security Intelligence Service

September 2017

## Appendix One: 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 1993
- 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, 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

---

### Draft Overseas Cooperation MPS NGO Consultation Document

# Consultation on the Review of the Ministerial Policy Statement on Cooperation of New Zealand Intelligence and Security Agencies (GCSB and NZSIS) with Overseas Public Agencies

On behalf of Hon Andrew Little, the Minister Responsible for the GCSB and the NZSIS, the Department of the Prime Minister and Cabinet is engaging in targeted consultation with relevant organisations to understand their views in the review of the Ministerial Policy Statement on cooperation of New Zealand intelligence and security agencies with overseas public agencies (Overseas Cooperation MPS).

## Background

### *Ministerial Policy Statements (MPSs)*

The [Intelligence and Security Act 2017](#) requires that the Minister responsible for the intelligence and security agencies issue MPSs in relation to the lawful activities of the agencies that set out any:

- procedures of an intelligence and security agency for authorising the carrying out of an activity relating to a matter
- protections that need to be in place in relation to the matter
- restrictions in relation to the matter.

The MPSs, reviewed and re-issued every three years, set out guiding principles that GCSB and NZSIS must apply when planning and carrying out these activities and identifies internal policies, procedures, consultation and training requirements in relation to each activity. The first MPSs were issued in 2017, and must be re-issued in 2020.

### *The Overseas Cooperation MPS*

The Intelligence and Security Act requires the Minister responsible for the GSCB and NZSIS to issue guidance to these agencies on:

- Co-operating with an overseas public authority
- Providing advice and assistance to an overseas public authority

- Sharing intelligence with an overseas public authority.

The first [Overseas Cooperation MPS](#) was issued in 2017. The MPS provides guidance for the GCSB and NZSIS in relation to all forms of cooperation with overseas public authorities<sup>1</sup>. It states that, when making decisions related to foreign cooperation the agencies must have regard to the principles of legality, human rights obligations, necessity, reasonableness and proportionality, protections for New Zealanders, information management, and oversight. It also sets out the procedures to authorise intelligence cooperation, assistance and sharing, and the protections and restrictions that need apply.

*Inspector-General of Intelligence and Security's Report into whether NZSIS and GCSB had any connection to the CIA's "enhanced interrogation", detention and rendition programme in Afghanistan between 2001-2009.*

In July 2019, the Inspector-General of Intelligence and Security (IGIS) released the report of her inquiry into whether New Zealand's intelligence and security agencies and personnel knew or were otherwise connected with, or risked connection to, the Central Intelligence Agency (CIA) detention and interrogation of detainees between 17 September 2001 and 22 January 2009 (accessible on the [IGIS website](#)).

In the IGIS' conclusions and recommendations, principal emphasis was placed on how the risks implicit in international intelligence-sharing and cooperation arrangements can best be anticipated and, where possible, be mitigated. The IGIS report recommended an early review of the Overseas Cooperation MPS<sup>2</sup> that consulted with relevant NGOs. The IGIS report noted this MPS had significant gaps regarding the clarity of limitations for information tainted by torture, and frameworks the agencies use in making decisions about when and how this information may or may not be used.

## Consultation Focus Areas and Questions

There are three particular areas that DPMC is seeking to consult on, on behalf of the Minister regarding the Overseas Cooperation MPS:

- How to clearly articulate the responsibilities and obligations relating to torture within the MPS (including torture's non-derogable nature).
- Defining exceptional circumstances, public emergencies and/or credible risks to national security where 'tainted' information, i.e. information likely obtained by torture, might be passed to relevant law enforcement agencies.
- How agencies should weigh up competing rights and interests, such as loss of life, significant personal injury, critical national infrastructure, and/or property.

---

<sup>1</sup> An overseas public authority is defined by the MPS as meaning a foreign person or body that performs or exercises an public function, duty, or power conferred on that person or body by or under law.

<sup>2</sup> The MPS, when issued in 2017, acknowledged the IGIS' ongoing work and anticipated that following the release of the IGIS report a review would need to be undertaken.

To explore these focus areas, consultees are invited to discuss the following questions alongside any general comments they wish to make on the Overseas Cooperation MPS:

1. Noting the focus areas of this consultation, whether the Overseas Cooperation MPS is consistent with relevant and/or applicable domestic and international legal principles?
2. Whether the Overseas Cooperation MPS provides appropriate clarity, alongside the Intelligence and Security Act 2017, regarding:
  - a. guidance to an intelligence and security agency for authorising the carrying out of an activity relating to cooperation with overseas public authorities.
  - b. protections that need to be in place in relation to the matter
  - c. restrictions in relation to the matter.
3. What level of protection should be afforded to property in the interests of national security? Should there be different levels of protection afforded to different types of (for example, comparing the rights of personal property and critical national infrastructure)?
4. Regarding information received by agencies that is likely to have been obtained by torture:
  - a. What might define exceptional circumstances, public emergencies or a credible national security threat that would justify an agency passing on that information?
  - b. What considerations, guidance or safeguards should the agencies apply when passing on that information?

## How to Respond

DPMC would appreciate written comments and responses to the questions above, if you wish to make them, to the questions above by [INSERT DATE]. Responses can be submitted via:

Email: [\[name.name\]@dpmc.govt.nz](mailto:[name.name]@dpmc.govt.nz)

Post: MPS Review  
National Security Group  
Department of the Prime Minister and Cabinet  
Level 8 Executive Wing  
Parliament Buildings  
Wellington.

If you wish to discuss your submission, please contact us via the email address above.



# Briefing

## PROPOSED REVISED APPROACH FOR REVIEWING THE MINISTERIAL POLICY STATEMENTS

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

Date	21/06/2020	Priority	Routine
Deadline	26/06/2020	Briefing Number	1920NSP/081

### Purpose

This briefing seeks your agreement to a revised approach to reviewing and re-issuing the Ministerial Policy Statements (MPSs), given the impact of the COVID-19 response on the review.


### Recommendations

1. **Note** that the Department of the Prime Minister and Cabinet is reviewing the MPSs on your behalf as part of the three year review cycle under the Intelligence and Security Act 2017 (the Act);
2. **Note** that the Act requires the MPSs to be reissued before September 2020;
3. **Note** that the pressures of the COVID-19 response has meant officials have been unable to progress the MPS review over the last three months;
4. **Agree** to the revised approach for reviewing the MPSs, including;
  - 4.1. Reviewing and reissuing six priority MPSs by September 2020;
  - 4.2. Reissuing the five remaining MPSs without review by September 2020; and
  - 4.3. Reviewing the remaining MPSs and reissuing all MPSs together by June 2021;

YES / NO



- 5. **Agree** to send the attached draft letter (Attachment A) to relevant ministers, outlining your proposed approach and inviting comment on any urgent concerns regarding the MPSs before they are reissued in September 2021; and YES / NO
  
- 6. **Agree** that we will engage the Inspector-General of Intelligence and Security on your behalf, outlining the proposed approach and invite comments on any urgent concerns regarding the MPSs before they are reissued in September 2021. YES / NO

  
Tony Lynch  
**Deputy Chief Executive  
National Security Group**

---

21.06.20  
...../...../.....

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	Team 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)	✓
Kaden Wilson	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

# PROPOSED REVISED APPROACH FOR REVIEWING THE MINISTERIAL POLICY STATEMENTS

## Purpose

1. This briefing seeks your agreement to a revised approach to reviewing and re-issuing the Ministerial Policy Statements (MPS), given the impact of the COVID-19 response on the review.

## We propose a revised, staged approach to reviewing the MPSs

2. You agreed in October 2019 that DPMC would lead the review and reissue of the MPSs on your behalf. The MPSs are required under the Intelligence and Security Act 2017 (the Act) to set out the responsible Minister's expectations of the GCSB and NZSIS and to provide guidance to the agencies on how certain lawful activities should be carried out. The Act requires the MPSs to be reissued by September 2020.
3. The Act does not specifically require the MPSs are reviewed prior to being reissued. However, as these are the first MPSs to be issued under the Act we proposed a detailed review to ensure they are workable, effective and did not have unforeseen consequences.
4. The response to COVID-19 has had a significant impact on the resources of DPMC and the agencies contributing to the review, which means we are unable to complete the review of all 11 MPSs by September 2020. Therefore we propose the following revised approach:

Timeline	Stage	MPSs ( <i>current status</i> )
<b>By September 2020</b>	<ol style="list-style-type: none"><li>1. Review and reissue six priority MPSs.</li></ol> <p><i>These six MPSs have either been identified by DPMC, GCSB and NZSIS as a priority for review (MPSs 4 and 6) or the review of the MPS is already underway</i></p>	<ol style="list-style-type: none"><li>1. Conducting activities with an exemption from the land transport (Road User) rule 2004 (<i>ready to reissue</i>);</li><li>2. Conducting surveillance in a public place (<i>MPS ready for Ministerial consultation – briefing attached</i>);</li><li>3. Collecting information lawfully from persons without a warrant or authorisation (<i>inter-agency consultation</i>);</li><li>4. Obtaining and using publicly available information (<i>inter-agency consultation</i>);</li><li>5. Requesting information from agencies under section 121 of the Intelligence and Security Act 2017 (<i>Inter-agency consultation</i>); and</li><li>6. Cooperation of New Zealand intelligence and security agencies (GCSB and NZSIS) with overseas public authorities (<i>Public consultation complete, Inter-agency consultation to begin</i>).</li></ol>

	<p>2. Reissue five remaining MPSs without review</p> <p><i>These five MPSs are not considered by DPMC, GCSB and NZSIS to have any urgent matters that need to be addressed prior to September 2020.</i></p>	<p>1. Acquiring, using and maintaining an assumed identity;</p> <p>2. Creating and maintaining a legal entity;</p> <p>3. Making false or misleading representations about being employed by an intelligence and security agency;</p> <p>4. Management of information obtained by an intelligence or security agency; and</p> <p>5. Providing information assurance and cyber security activities with consent.</p>
By June 2021	3. Review the five remaining MPSs	As above.
	4. Reissue all reviewed MPSs	All MPSs realigned to the same three year review timeline.

5. This proposal balances the requirements of the Act while effectively using the time available to address priorities we have identified in conversations with the GCSB and NZSIS. It will also re-align all MPSs to the same three year cycle for reissue, and has the added advantage of de-coupling the MPS review from future General Election timing.
6. We do not consider there are any risks with delaying the review of the five remaining MPSs by eight months. The GCSB and NZSIS have confirmed there are no immediate issues with the five MPSs for reissue that need addressing prior to September 2020.
7. Given the complexity of the issues within the *Cooperation of New Zealand intelligence and security agencies (GCSB and NZSIS) with overseas public authorities* MPS, there is a chance that the review of this MPS may not be completed by September 2020. We will keep your office informed if there are any delays with this review.

## Next Steps

8. Given the requirement under the Act to consult with Ministers whose areas of responsibility includes an interest in an MPS, as well as the Inspector-General of Intelligence and Security (the IGIS), we recommend that, as a courtesy, you update them on the proposed approach. To support you in this, we propose that:
  - a) You send the attached draft letter (**Attachment A**) to relevant Ministers<sup>1</sup> outlining your approach, inviting urgent comments on MPSs that relate to their portfolio which will not be reviewed before September 2020; and

<sup>1</sup> Relevant Ministers include the Minister of Internal Affairs, Hon Tracey Martin; Minister of Police, Hon Stuart Nash; Minister of Transport, Hon Phil Twyford; Minister of Broadcasting, Communications and Digital Media, Hon Kris Faafoi; Minister of Customs, Hon Jenny Salesa; Minister of Defence, Hon Ron Mark.

- b) We engage the IGIS on your behalf (as part of our wider support on the review of the MPSs) and invite urgent comments on any MPS that will not be reviewed before September 2020.
- 9. We will also work with your office on decisions needed in relation to the six MPSs to be reviewed by September 2020.

<b>Attachments:</b>		
<b>Attachment A:</b>	Unclassified	Draft letter to relevant Ministers regarding revised MPS review timeline and seeking comments on urgent matters

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

# ATTACHMENT A

Hon [Minister Name]  
[Role Title]  
Parliament Buildings

Dear Minister [Name]

## Revised Timeline for the Review and Reissue of the Ministerial Policy Statements

Sections 206 and 207 of the Intelligence and Security Act 2017 (the Act) requires the Minister(s) responsible for the intelligence and security agencies to issue Ministerial Policy Statements (MPSs) about certain lawful activities carried out by the GCSB and the NZSIS.

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 Responsible Minister for both the GCSB and the NZSIS, I am responsible for reviewing and reissuing the MPSs.

The current 11 MPSs are required to be reissued within three years from the September 2017 date they took effect. 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.

My intention had been to review and reissue all MPSs by September 2020. However, in light of the challenges with Government agencies responding to COVID-19 I have now reconsidered this approach. My priority now is to review six of the MPSs, and reissue the remaining five MPSs without review prior to the September 2020 statutory deadline.<sup>2</sup> This will mean that the following five MPSs will be reissued without review:

1. Acquiring, using and maintaining an assumed identity;
2. Creating and maintaining a legal entity;
3. Making false or misleading representations about being employed by an intelligence and security agency;
4. Management of information obtained by an intelligence or security agency; and
5. Providing information assurance and cyber security activities with consent.

There are not thought to be any issues with these MPSs that need to be addressed urgently. I plan to review and reissue these five MPSs by mid-2021. In the interim, if you consider there are any urgent matters that should be addressed prior to their reissue I recommend your officials make contact with my officials by 10 July 2020 to discuss.

Yours sincerely

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

---

<sup>2</sup> For the six MPSs that will be reviewed before September 2020, I will consult you as appropriate for comment on MPSs relevant to your portfolio.



# Briefing

## CONSULTATION ON MINISTERIAL POLICY STATEMENT: CONDUCTING SURVEILLANCE IN A PUBLIC PLACE

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

Date	22/06/2020	Priority	Routine
Deadline	26/06/2020	Briefing Number	1920NSP/054

### Purpose


This briefing outlines the proposed changes to the draft Ministerial Policy Statement (MPS): *Conducting surveillance in a public place*, following its recent review. To support the Ministerial consultation that you are required to do under the Intelligence and Security Act 2017, it also attaches draft letters and a revised draft of the MPS, for forwarding to:

- Hon Stuart Nash, Minister of Police and Minister of Fisheries
- Hon Jenny Salesa, Minister of Customs
- Hon Damien O'Connor, Minister of Agriculture and Minister for Biosecurity.

### Recommendations

1. **Note** that the Department of the Prime Minister and Cabinet is reviewing the Ministerial Policy Statements under the Intelligence and Security Act 2017 on your behalf
2. **Note** that we propose changes to the Ministerial Policy Statement: *Conducting surveillance in a public place*
3. **Note** that under the Intelligence and Security Act 2017, you are required to consult relevant Ministers as the Ministerial Policy Statements are reviewed and reissued
4. **Agree** to sign and forward the attached letters and draft Ministerial Policy Statement: *Conducting surveillance in a public place* to:
  - 4.1 Hon Stuart Nash, Minister of Police and Minister of Fisheries **YES / NO**
  - 4.2 Hon Jenny Salesa, Minister of Customs **YES / NO**

4.3 Hon Damien O'Connor, Minister of Agriculture and Minister for Biosecurity. YES / NO

 Tony Lynch <b>Deputy Chief Executive National Security Group</b>
22 06 20 ...../...../.....

Hon Andrew Little <b>Minister Responsible for the GCSB Minister Responsible for the NZSIS</b>
...../...../.....

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982



Contact for telephone discussion if required:

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

# CONSULTATION ON MINISTERIAL POLICY STATEMENT: CONDUCTING SURVEILLANCE IN A PUBLIC PLACE

## Purpose

---

1. This briefing outlines the proposed changes to the draft Ministerial Policy Statement: *Conducting surveillance in a public place*, following its recent review. To support the Ministerial consultation that you are required to do under the Intelligence and Security Act 2017, it also attaches draft letters and a revised draft of the Ministerial Policy Statement (MPS) for forwarding to:
  - Hon Stuart Nash, Minister of Police and Minister of Fisheries
  - Hon Jenny Salesa, Minister of Customs
  - Hon Damien O'Connor, Minister of Agriculture and Minister for Biosecurity

## Review of the MPS

---

2. To review this MPS we worked with NZSIS on whether the MPS provided clear and appropriate guidance in relation to conducting surveillance in a public place. We looked at how the NZSIS had incorporated the MPS into its operations and whether there were any problems with the MPS. We also consulted with:
  - The Acting Inspector-General of Intelligence and Security
  - The Privacy Commissioner
  - The Ministry of Justice
  - New Zealand Police
  - New Zealand Customs
  - The Ministry for Primary Industries.

## Proposed changes to the MPS

---

3. Key feedback on this MPS was that generally it provided clear guidance to the NZSIS, but there were parts that caused confusion and could be made clearer. As a result we propose the following changes:
  - a) Revise the "use of equipment" section. The NZSIS reported that this section created confusion as to what type of equipment or technology could be used when conducting surveillance in a public place without a warrant. This resulted in avoidable checks with the legal team and sometimes ceasing operations while these checks were made. We have renamed this section "use of technology" and added language that emphasises only technology that enhances imagery already within public view are to be used.
  - b) Add further context on when NZSIS might conduct surveillance in a public place, including when the NZSIS is undertaking preliminary inquiries.
  - c) Revise the section on legality to make it clearer when surveillance in a public place is clearly lawful.

- d) Add further context to the “respect for privacy” principle. We have expanded on the separate factors to be considered when assessing privacy aspects, such as the location and duration of the surveillance, the observation of third parties not under surveillance, and the nature of activities being observed. The discussion on the preference to use less intrusive means where possible was also strengthened.
  - e) Simplify the language on implied licence. Implied licence is a difficult concept in respect of conducting surveillance in a public place, so we have simplified this language and NZSIS will provide more guidance in their internal operational documentation.
  - f) Under the “Matters to be reflected in internal policies and procedures” section, we have decoupled the “Communications protected by privilege” from the “sensitive category individuals”. This is to recognise the unique characteristics of each group that should be considered by NZSIS’s internal procedures and policies.
  - g) Revise the use of examples within the MPS. The previous version of the MPS included examples that were repetitive and sometimes not relevant to the context. We have streamlined the examples and used more relevant examples provided by the operational teams in NZSIS.
  - h) Minor changes to reduce repetition and improve readability.
4. The revised draft Ministerial Policy Statement: *Conducting surveillance in a public place*, with highlighted changes, is attached (**Attachment A**). A clean version of the MPS is also attached (**Attachment B**).

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

---

5. Under Section 212 of the Intelligence and Security Act 2017 (the Act), you are required to consult with any other Minister of the Crown whose area of responsibility includes an interest in the proposed MPS.
6. In this case, we recommend you consult with Hon Stuart Nash – Minister of Police and Minister of Fisheries, Hon Jenny Salesa – Minister of Customs, and Hon Damien O’Connor – Minister of Agriculture and Minister for Biosecurity. These portfolios were consulted on the original MPS as their respective agencies conduct surveillance in public places, and to help ensure consistency in this activity across government.
7. Draft letters to these Ministers are attached as Attachments C, D and E, for your signature. You may also wish to consider the revised MPS in your capacity as Minister of Justice.

## Next Steps

---

8. Once you receive any feedback on the MPS from Ministerial consultation, we will support you in adapting the MPS to reflect the comments.
9. Revision of the Ministerial Policy Statement: *Conducting surveillance in a public place* is part of a programme of work to review all eleven MPSs. We have prepared an accompanying briefing (1920NSP/081) seeking your agreement to a revised approach to reviewing the MPS given the delays caused by the COVID-19 response.

Attachments:		
<b>Attachment A:</b>	Unclassified	Draft revised Ministerial Policy Statement: <i>Conducting Surveillance Public Surveillance</i> – marked-up version
<b>Attachment B:</b>	Unclassified	Draft revised Ministerial Policy Statement: <i>Conducting Surveillance Public Surveillance</i> – clean version
<b>Attachment C:</b>	Unclassified	Letter to Hon Stuart Nash, Minister of Police and Minister of Fisheries
<b>Attachment D:</b>	Unclassified	Letter to Hon Jenny Salesa, Minister of Customs
<b>Attachment E:</b>	Unclassified	Letter to Hon Damien O'Connor, Minister of Agriculture and Minister for Biosecurity

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

## Attachment A

---

**Draft revised Ministerial Policy Statement: Conducting surveillance in a public place** (*marked-up version*)

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

## Attachment B

---

**Draft revised Ministerial Policy Statement: Conducting surveillance in a public place** (*clean version*)

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

## Attachment C

---

Hon Stuart Nash  
Minister of Police  
Minister of Fisheries  
Parliament Buildings

Dear Minister Nash

### **Consultation on ministerial policy statement: Conducting Surveillance in a Public Place**

I enclose for your comment a draft of the revised Ministerial Policy Statement: *Conducting Surveillance in a Public Place* by intelligence agencies under subpart 2 of Part 3 of the Intelligence and Security Act 2017 (the Act).

Sections 206 and 207 of the Act require the Minister(s) responsible for the intelligence and security agencies to issue Ministerial Policy Statements (MPSs) about certain lawful activities carried out by the GCSB and the NZSIS. 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 Responsible Minister for both 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 is relevant to your portfolio responsibilities both as Minister of Police and as Minister of Fisheries. The agencies within these portfolios also conduct surveillance in public places and it is important there is consistency across government in undertaking this activity.

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, DPMC has consulted with the Inspector-General of Intelligence and Security, the Ministry of Justice, Ministry for Primary Industries, New Zealand Police, New Zealand Customs Service and the Privacy Commissioner. The consultation has shown that while overall the MPS provides clear guidance to the NZSIS in conducting surveillance in a public place, parts of the MPS caused confusion and could be made clearer. The attached MPS highlights the proposed changes.

If you have any comments, I would be grateful to receive these by 10 July 2020.

Yours sincerely

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

Attachment: Draft Ministerial Policy Statement: Conducting surveillance in a public place (*marked-up version*)

Attachment: Draft Ministerial Policy Statement: Conducting surveillance in a public place (*clean version*)

## Attachment D

---

Hon Jenny Salesa  
Minister of Customs  
Parliament Buildings

Dear Minister Salesa

### **Consultation on ministerial policy statement: Conducting Surveillance in a Public Place**

I enclose for your comment a draft of the revised Ministerial Policy Statement: *Conducting Surveillance in a Public Place* by intelligence agencies under subpart 2 of Part 3 of the Intelligence and Security Act 2017 (the Act).

Sections 206 and 207 of the Act require the Minister(s) responsible for the intelligence and security agencies to issue Ministerial Policy Statements (MPSs) about certain lawful activities carried out by the GCSB and the NZSIS. 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 responsible Minister for both 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 is relevant to your portfolio responsibilities as Minister of Customs. NZ Customs also conducts surveillance in public places and it is important there is consistency across government in undertaking this activity.

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, DPMC has consulted with the Inspector-General of Intelligence and Security, the Ministry of Justice, Ministry for Primary Industries, New Zealand Police, New Zealand Customs Service and the Privacy Commissioner. The consultation has shown that while overall the MPS provides clear guidance to the NZSIS in conducting surveillance in a public place, parts of the MPS caused confusion and could be made clearer. The attached MPS highlights the proposed changes.

If you have any comments, I would be grateful to receive these by 10 July 2020.

Yours sincerely

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

Attachment: Draft Ministerial Policy Statement: Conducting surveillance in a public place (*marked-up version*)

Attachment: Draft Ministerial Policy Statement: Conducting surveillance in a public place (*clean version*)



## Attachment E

---

Hon Damien O'Connor  
Minister of Agriculture  
Minister for Biosecurity  
Parliament Buildings

Dear Minister O'Connor

### **Consultation on ministerial policy statement: Conducting Surveillance in a Public Place**

I enclose for your comment a draft of the revised Ministerial Policy Statement: *Conducting Surveillance in a Public Place* by intelligence agencies under subpart 2 of Part 3 of the Intelligence and Security Act 2017 (the Act).

Sections 206 and 207 of the Act require the Minister(s) responsible for the intelligence and security agencies to issue Ministerial Policy Statements (MPSs) about certain lawful activities carried out by the GCSB and the NZSIS. 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 both 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 is relevant to your portfolio responsibilities both as Minister of Agriculture and Minister for Biosecurity. The agencies within these portfolios also conduct surveillance in public places and it is important there is consistency across government in undertaking this activity.

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, DPMC has consulted with the Inspector-General of Intelligence and Security, the Ministry of Justice, Ministry for Primary Industries, New Zealand Police, New Zealand Customs Service and the Privacy Commissioner. The consultation has shown that while overall the MPS provides clear guidance to the NZSIS in conducting surveillance in a public place, parts of the MPS caused confusion and could be made clearer. The attached MPS highlights the proposed changes.

If you have any comments, I would be grateful to receive these by 10 July 2020.

Yours sincerely

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

Attachment: Draft Ministerial Policy Statement: Conducting surveillance in a public place (*marked-up version*)

Attachment: Draft Ministerial Policy Statement: Conducting surveillance in a public place (*clean version*)



# Briefing

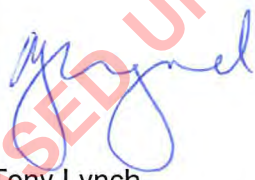
## REVIEW OF THE MINISTERIAL POLICY STATEMENTS – REVISED TIMING

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

Date	28/08/2020	Priority	Routine
Deadline	13/09/2020	Briefing Number	2021NSP/010

### Recommendations

1. **Note** that, in July 2020, you agreed to a revised approach to reviewing and reissuing the Ministerial Policy Statements, given the significant impact of the COVID-19 response on the review;
2. **Note** that there have been further delays, meaning we are unable to complete the review of six of the 11 MPSs by September 2020;
3. **Agree** to reissue the MPSs as they stand prior to 28 September 2020; **YES / NO**
4. **Agree** to the MPSs being reviewed and reissued prior to June 2021. **YES / NO**

  
 Tony Lynch  
 Deputy Chief Executive  
 National Security Group

28/08/20  
 ...../...../.....

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	Team 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

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

# REVIEW OF THE MINISTERIAL POLICY STATEMENTS – REVISED TIMING

## Purpose

---

1. This briefing seeks your agreement to a revised timeline for reviewing the Ministerial Policy Statements (MPSs).

## The Ministerial Policy Statements are required to be re-issued by September 2020

---

2. The Department of the Prime Minister and Cabinet, working closely with GCSB and NZSIS, is leading the review of the MPSs on your behalf. There are 11 MPSs which set out the responsible Minister's expectations and provide guidance to the GCSB and NZSIS on how certain lawful activities should be carried out.
3. The Intelligence and Security Act 2017 (the Act) requires the MPSs to be reissued by 28 September 2020. While the Act does not specifically require the MPSs to be reviewed prior to being reissued, given these were the first MPSs to be issued under the Act we proposed a detailed review to ensure the MPSs were workable and effective.

## The response to COVID-19 meant the review was delayed

---

4. In July 2020, you agreed to a revised approach to reviewing and reissuing the MPSs, given the significant impact of the COVID-19 response on the review [1920NSP/081 refers]. At that time we had proposed to:
  - By end-September 2020:
    - review and reissue six MPSs;
    - reissue the five remaining MPSs without review.
  - By end-June 2021:
    - Review the remaining five MPSs;
    - Reissue all reviewed MPSs (so all MPSs were aligned to the same three-year review period).
5. At this stage, we have completed the review of two MPSs. There have been further delays with the review of the other four MPSs we had hoped to complete by September. As highlighted in the previous briefing, these are the more complex MPSs and it has taken time to resolve a number of issues, alongside competing priorities within each of the responsible agencies. This means we are not able to meet the statutory requirement to consult with Ministers and the Inspector-General of Intelligence and Security (IGIS) in the required timeframe.
6. In addition, the IGIS is reviewing GCSB and NZSIS's open source activities, including how the agencies apply the guidance in the relevant MPS ('Obtaining and using publicly

available information'). We would like to wait for the outcome of that review (expected to be completed in October 2020) before finalising the review of this MPS.

7. Re-issuing the MPSs at a later date will also enable us to incorporate any recommendations from the Royal Commission of Inquiry into the Attack on Christchurch Mosques.

## **We now propose to review and re-issue the Ministerial Policy Statements by June 2021**

---

8. GCSB, NZSIS and the IGIS have confirmed there are no immediate issues that need addressing prior to the MPSs being reissued by end-September 2020, as required by the ISA. We are still on track to review the remaining nine MPSs and to reissue all 11 MPSs by June 2021.
9. We do not consider there are any risks with reviewing and reissuing the MPSs by June 2021. Reissuing all MPSs together at this time has the advantage of decoupling the MPS reviews with future General Election timings.

### **However we intend to re-issue the MPS on Overseas Cooperation prior to June 2021**

10. The one exception to this timing is the MPS on 'Cooperation of New Zealand intelligence and security agencies (GCSB and NZSIS) with overseas public authorities', which we are currently reviewing and intend to re-issue as soon as possible.
11. The IGIS has recommended early review of this MPS in the report *Inquiry into possible New Zealand intelligence and security agencies' engagement with the CIA detention and interrogation programme* (the Senate Report). The agencies are seeking the Overseas Cooperation MPS review to be finalised prior to their review of the Joint Policy Statement on Human Rights Risk Management, which was also a recommendation in the Senate Report.

## **Next steps**

---

12. If you agree with the revised approach set out in this briefing, we will provide you with the 11 MPSs to reissue prior to end-September 2020.
13. We will work with your office on decisions needed in relation to the ongoing review.

## **Consultation**

---

14. GCSB and NZSIS were consulted on this briefing and have given their commitment to completing the review in the revised timeframe. The Office of the IGIS has been consulted on the revised timing and has confirmed they can manage their resourcing to support the timing of the review.

# Briefing

## CONSULTATION ON MINISTERIAL POLICY STATEMENT: COOPERATING WITH OVERSEAS PUBLIC AUTHORITIES

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

Date	18/12/2020	Priority	Routine
Deadline	18/01/2021	Briefing Number	2021NSP/030

### Purpose

This briefing outlines the proposed changes to the draft Ministerial Policy Statement (MPS): *Cooperating with overseas public authorities*, following its recent review.

To support the Ministerial consultation you are required to do under the Intelligence and Security Act 2017, it also attaches draft letters and a revised draft of the MPS, for forwarding to:

- Hon Nanaia Mahuta, Minister of Foreign Affairs;
- Hon Poto Williams, Minister of Police;
- Hon Kris Faafoi, Minister of Justice and Minister of Immigration;
- Hon Peeni Henare, Minister of Defence;
- Hon Meka Whaitiri, Minister of Customs.

### Recommendations

1. **Approve** the draft revised Ministerial Policy Statement (MPS): Cooperating with overseas public authorities (Attachment B) for ministerial consultation; **YES / NO**

2. **Agree** to provide additional guidance to the Directors-General on the following matters via a letter when the MPS is reissued:

2.1 s6(a)  **YES / NO**

2.2 s6(a) [Redacted] YES / NO

3. **Note** that under the Intelligence and Security Act 2017, you are required to consult relevant Ministers as the Ministerial Policy Statements are reviewed and reissued;

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

4.1 Hon Nanaia Mahuta, Minister of Foreign Affairs; YES / NO

4.2 Hon Poto Williams, Minister of Police; YES / NO

4.3 Hon Kris Faafoi, Minister of Justice and Minister of Immigration; YES / NO

4.4 Hon Peeni Henare, Minister of Defence; YES / NO

4.5 Hon Meka Whaitiri, Minister of Customs. YES / NO



Tony Lynch  
**Deputy Chief Executive  
 National Security Group  
 Department of the Prime Minister and  
 Cabinet**

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

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

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982



# CONSULTATION ON MINISTERIAL POLICY STATEMENT: COOPERATING WITH OVERSEAS PUBLIC AUTHORITIES

## Purpose

---

1. This briefing outlines the proposed changes to the *draft Ministerial Policy Statement (MPS): Cooperating with overseas public authorities*, following its recent review. To support the Ministerial consultation 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:
  - Hon Nanaia Mahuta, Minister of Foreign Affairs;
  - Hon Poto Williams, Minister of Police;
  - Hon Kris Faafoi, Minister of Justice and Minister of Immigration;
  - Hon Peeni Henare, Minister of Defence;
  - Hon Meka Whaitiri, Minister of Customs.

## Executive Summary

---

2. The Department of Prime Minister and Cabinet, working closely with GCSB and NZSIS, has reviewed the *MPS: Cooperating with overseas public authorities* (the overseas cooperation MPS) on your behalf.
3. We consulted widely on this MPS, with government agencies, the Inspector-General of Intelligence and Security (IGIS), the Human Rights Commission, Office of the Privacy Commissioner, and NGOs. As a result we propose a number of changes to the MPS, including:
  - restructuring it to include a 'cover sheet' that sets out the overarching purpose of the MPSs which will be common across all 11 MPSs
  - clarifying it only applies to lawful activity
  - including a human rights risk assessment framework
  - providing consistency in assessing risk
  - adding detail on the exceptional circumstances in which the agencies can use intelligence where they know or assess the intelligence was obtained through a serious human rights breach.
4. The revised MPS is attached, for you to consult with relevant Ministerial colleagues as you are required to do under the Act. Once you receive any feedback from this consultation, we will adapt the MPS to reflect the comments. The MPS can then be finalised and reissued. At that point, a copy of the MPS must be provided to the Intelligence and Security Committee (ISC), as per section 207(2) of the Act.

## **DPMC is reviewing the MPSs on your behalf**

---

5. Under the Act the MPSs are required to be reissued every three years. DPMC, working closely with GCSB and NZSIS, is reviewing the MPSs on your behalf.
6. Due to disruptions caused by COVID-19, the work in preparation for the Royal Commission of Inquiry into the Christchurch attacks and other competing priorities, the MPSs were reissued without review in September 2020. We are now aiming to review and reissue all MPSs prior to June 2021.

## **Review of the overseas cooperation MPS**

---

7. The purpose of the overseas cooperation MPS is to set out your expectations, as the responsible Minister, for how the GCSB and NZSIS properly cooperate with overseas public authorities. The MPS provides a framework for decision-making and best practice conduct for the agencies when undertaking foreign cooperation – which includes providing advice and assistance, and sharing intelligence.
8. Given the significant focus on human rights in the MPS, there has been a strong level of interest in the review from other government agencies, the Inspector-General of Intelligence and Security (IGIS) and NGOs who promote human rights. To reflect this level of interest, the review has been comprehensive and in-depth, with levels of consultation and engagement beyond that of the other MPSs we are reviewing on your behalf.

### **We worked closely with GCSB and NZSIS**

9. We worked closely with the policy, legal and operational branches of GCSB and NZSIS on the review of this MPS to consider:
  - whether the MPS provided clear guidance to the agencies when cooperating with overseas public authorities;
  - how the MPS was incorporated into the operations of the agencies and whether there were any impediments to the operationalisation of the MPS;
  - any unintended consequences, or other issues, including on the effectiveness and efficiency of the agencies; and
  - the comments and views of relevant oversight bodies, including the Inspector-General of Intelligence and Security (IGIS) and Government agencies.
10. As we revised the MPS we consistently checked in with the agencies against these points, to ensure any revisions were operationally workable. GCSB and NZSIS were given the opportunity to respond to comments made by other parties during the consultation process.

### **We considered the recommendations of the IGIS report**

11. The 2019 IGIS report: *Inquiry into possible New Zealand intelligence and security agencies' engagement with the CIA detention and interrogation programme 2001-2009* (the IGIS report) made several recommendations to address gaps the IGIS identified in this MPS.
12. The IGIS report stated that the MPS should unambiguously set out New Zealand's legal obligations relating to torture and complicity in torture. This was not able to be achieved

when the MPS was developed in 2017. The Ministry of Foreign Affairs and Trade (MFAT) has since issued a legal opinion to clarify New Zealand's obligation, at international law, not to be complicit in an internationally wrongful acts of another State. This opinion informed the review of the MPS, however the guidance in the MPS sets a higher policy threshold than the legal threshold of complicity.

13. The IGIS report also identified the following gaps in the 2017 MPS:

- it does not state that the prohibition of torture is non-derogable (ie it cannot be lifted in any circumstance);
- it does not specify the circumstances in which the use of 'tainted' information might be justified;
- it accorded property primacy over protecting human rights;
- the threats or risks that, when identified, would allow the agencies to share information through human rights abuses, lack clarity;
- there is inconsistency in whether 'tainted' information may or should be passed to relevant law enforcement agencies;
- it is unclear what 'unsolicited' means in the context of an intelligence-sharing relationship and why the distinction is necessary; and
- the MPS refers to situations where intelligence that indicates a 'credible' security risk is suspected to have been gained through torture, which does not reconcile with the statement that information gained by torture is inherently unreliable.

14. We worked closely with the Office of the IGIS as we revised the MPS, to check that the revisions sufficiently addressed the recommendations made in the IGIS Report, and to seek their views on whether the MPS provided appropriate guidance to the agencies from the perspective of their oversight role. This consultation undertaken on your behalf has fulfilled your obligation under the Act to consult the IGIS when reviewing and updating the MPS. The IGIS is satisfied with the current draft, thinks it is an improvement from the 2017 MPS, and considers we have addressed all of the concerns their office has raised.

### **We consulted with key NGOs**

15. One of the recommendations from the IGIS report was to consult with key NGOs on the revised MPS. You agreed that we would consult with a small number of organisations that promote and defend human rights, and understand New Zealand's international human rights obligations [1920NSP/031 refers]. Earlier in the year, we contacted five organisations<sup>1</sup> to seek their feedback on the MPS, including in particular:

- how to clearly articulate human rights responsibilities and obligations within the MPS;
- defining exceptional circumstances at which information likely obtained by torture might be passed to law enforcement agencies;

---

<sup>1</sup> Amnesty International, Privacy International, New Zealand Council for Civil Liberties, Human Rights Foundation and the Privacy Foundation

- whether the MPS was consistent with domestic and international human rights obligations; and
  - whether the MPS provided appropriate clarity regarding guidance, protections and restrictions in cooperating with overseas public authorities.
16. The Privacy Foundation was the only organisation that responded to the consultation document. The other organisations appreciated being consulted, and either had no comments or were unable to prioritise providing feedback, including after the deadline was extended due to COVID-19.
17. The Privacy Foundation made a number of recommendations related to the adequacy of the MPS in relation to human rights obligations, improvements to provide more clarity on the guidance, safeguards and restrictions needed to for cooperation to occur, and suggestions on the level of protection afforded to property in connection with national security. This feedback was reflected in the revised draft of the MPS.

### **We also consulted key government departments**

18. We also consulted with the following agencies with an interest in this MPS:
- The Ministry of Foreign Affairs and Trade;
  - The Ministry of Justice;
  - The Privacy Commissioner;
  - The Human Rights Commission;
  - New Zealand Police;
  - New Zealand Customs;
  - The Ministry of Defence;
  - The New Zealand Defence Force.
19. We consulted with these agencies on the first revised draft of the MPS. These agencies were also given an opportunity to provide feedback on a second revised draft. If any feedback was not taken on board, we provided justification for this that agencies have accepted.
20. Overall, agencies noted that this review has significantly improved the MPS. The Human Rights Commission (HRC) is the main agency that provided feedback we did not incorporate into the draft MPS:
- They suggested the definition of 'overseas public authorities' be expanded to include private contractors and agents of these authorities. We did not think this was necessary as the definition in the Act includes any person working for the public authority.
  - They suggested authorisation for overseas cooperation is provided by an external independent body. This is beyond the scope of the MPS review and would require legislative change.

- Both the HRC and the IGIS recommended that the agencies' internal human rights policy should be made public. DPMC's view is that the agencies' internal policy needs to provide detailed and frank guidance to staff on assessing human rights risk. If the agencies draft their internal policies with the intention of those documents becoming public, this would detract from their primary purpose and mean they are less useful to staff.
- HRC suggested requiring the agencies to develop a policy to state how they will monitor partner countries, and require them to review certain countries every six months. The MPS sets out the matters the agencies need to consider when reviewing the human rights practices of a country. Requiring the agencies to review every six months has unjustified resource implications.

21. Our understanding is that, apart from these matters, there are no outstanding substantial differences in views.

### **Proposed changes to the MPS**

22. The following table sets out the substantive changes to the MPS. There are also a number of more minor changes, including to the structure, to improve readability and consistency and reduce repetition.

**Table One: Substantive changes to the MPS**

<b>Change</b>	<b>Recommended by</b>
1. The structure has been changed to include a cover sheet (or website landing page) which will become common across all of the MPSs. This sets out the overarching purpose of the MPSs, so each individual MPS focuses on the specific activity (in this case overseas cooperation)	DPMC, GCSB, NZSIS, IGIS
2. The MPS now makes it clearer that it only applies to lawful activity, and is not a framework for what is or is not lawful. The legality principle has been removed and it is instead set out in the scope section that it only applies to lawful activity and if in doubt, legal advice should be sought. This will also now be common across all MPSs (as appropriate).	MFAT, IGIS, MoJ, GCSB, NZSIS
3. The MPS now includes a risk assessment framework to be reflected in the agencies' internal policies 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 has been informed by MFAT's advice and the IGIS report – which were both developed since 2017.	IGIS
4. Consistent language is used throughout on the threshold of assessing risk – where there is a 'real risk' of contributing to a human rights breach.	IGIS, DPMC, GCSB, NZSIS
5. It now includes detail of the exceptional circumstances in which agencies can use intelligence where they know or assess there was a real risk that the intelligence was obtained through a serious human rights breach. That is, where the use of the intelligence is necessary to prevent loss of life, significant personal injury or a threat to critical national infrastructure.	IGIS, Privacy Foundation, GCSB, NZSIS

6. Added in text to address situations where cooperation may result in a person being sentenced to death.	MFAT, NZ Customs
7. The MPS now states that the prohibition of torture is non-derogable.	IGIS, Privacy Foundation
8. The MPS now includes criteria that the agencies need to take into account when considering whether to refer a written arrangement to the Intelligence and Security Committee (ISC).	DPMC, IGIS, GCSB, NZSIS

**When the MPS is reissued, we recommend two matters are clarified**

23. There are two further matters in which the agencies sought clarification in the review of this MPS which require further explanation:

a. s6(a)



b. The guidance in the current MPS on when the agencies should refer a written arrangement with an overseas public authority to the ISC is open to interpretation, and as a result no arrangements have been referred in the past three years. We have therefore included criteria to assist in the determination of what arrangements should be referred to the ISC, namely where the arrangement:

- 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.

s6(a)



The agencies will apply the revised MPS criteria for referral of arrangements retrospectively to written arrangements entered into since 2017.

24. If you wish to provide additional guidance to the agencies on these matters, DPMC will provide suggested wording for inclusion in the letters to the Directors-General when the MPS is reissued.

## Next Steps

---

25. 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.
26. The ministerial consultation is not urgent and you may choose to consult in early 2021.
27. Once you receive any feedback from your consultation, we will adapt the MPS to reflect the comments. The MPS can then be finalised and reissued. The Act then requires you to provide a copy to the ISC.

Attachments:		
<b>Attachment A:</b>	Unclassified	Draft revised Ministerial Policy Statement: <i>Cooperating with overseas public authorities</i>
<b>Attachment B</b>	Unclassified	2017 version of Ministerial Policy Statement: <i>Cooperating with overseas public authorities</i>
<b>Attachment C:</b>	Unclassified	Letter to Hon Nanaia Mahuta, Minister of Foreign Affairs
<b>Attachment D:</b>	Unclassified	Letter to Hon Poto Williams, Minister of Police
<b>Attachment E:</b>	Unclassified	Letter to Hon Kris Faafoi, Minister of Justice and Minister of Immigration
<b>Attachment F:</b>	Unclassified	Letter to Hon Peeni Henare, Minister of Defence
<b>Attachment G:</b>	Unclassified	Letter to Hon Meka Whaitiri, Minister of Customs

# ATTACHMENT A

## DRAFT REVISED MINISTERIAL POLICY STATEMENT: COOPERATING WITH OVERSEAS PUBLIC AUTHORITIES

### *Ministerial Policy Statements*

1. Ministerial Policy Statements (MPSs) are statements issued by the Minister Responsible for the GCSB and NZSIS under section 206 and 207(1) of the Intelligence and Security Act 2017 (‘the Act’).

#### **MPSs provide guidance to GCSB and NZSIS on certain lawful activities**

2. MPSs provide guidance to GCSB and NZSIS (also called ‘the agencies’) on lawful activities under the Act. They do not act as legal authorisations for these activities but set out the Minister’s expectations of how the activities covered by the MPS should be properly carried out and any protections or restrictions in relation to the activity. Activities which are unlawful may only be carried out to the extent that they can be authorised under an intelligence warrant.
3. Every employee making decisions or taking any action in relation to the matters covered by the MPSs must consider and should be able to explain how they had regard to the MPS. This might include an explanation of the consideration of any relevant internal policy or procedures that reflect the MPS. The Directors-General of the GCSB and NZSIS are responsible for ensuring each MPS is reflected in their agency’s internal policies and procedures. If any action is taken that is inconsistent with the MPS, employees must be able to explain why that action was taken.

#### **They are also considered by the Inspector-General of Intelligence and Security when conducting an inquiry or review**

4. MPSs are relevant to the oversight of the agencies by the Inspector-General of Intelligence and Security in the exercise of their propriety jurisdiction. When conducting an inquiry or review, the Inspector-General of Intelligence and Security must take account of any relevant MPS and the extent to which an agency has complied with it.

#### **And they assist in increasing transparency with the New Zealand public**

5. While the primary purpose of the MPSs is to provide guidance to the agencies on their lawful activities, they also provide the public with information on how and why the agencies carry out these activities to help keep New Zealand secure.

#### **Each of the activities covered by the MPSs enable the agencies to perform their statutory functions**



6. The Act sets the principal objectives of GCSB and NZSIS, which are to contribute to:
  - The protection of New Zealand's national security;
  - The international relations and well-being of New Zealand; and
  - The economic well-being of New Zealand.
7. The GCSB and NZSIS meet these objectives through the performance of their statutory functions, namely:
  - Intelligence collection and analysis;
  - Protective security services, advice and assistance;
  - Cooperation with other public authorities to facilitate their functions; and
  - Cooperation with other entities to respond to imminent threat.
8. All collection and analysis of intelligence undertaken by GCSB and NZSIS is in accordance with the New Zealand Government's priorities. These are primarily established through the National Security and Intelligence Priorities (NSIPs) which are set by the Government and reviewed every two years. The NSIPs outline the focus areas for all intelligence and assessment activity across the national security sector, including GCSB and NZSIS.
9. MPSs are an important part of the measures put in place by the Act to ensure these functions are carried out properly.

#### **Matters covered by the MPSs**

10. The MPSs cover areas of work of the agencies that involve gathering information about individuals and organisations that may intrude into the privacy of individuals and other areas where ministerial guidance was considered appropriate. There are currently 11 MPSs, covering the following activities:
  1. Providing information assurance and cybersecurity activities;
  2. Acquiring, using and maintaining an assumed identity;
  3. Creating and maintaining a legal entity (such as a cover company);
  4. Collecting information lawfully from persons without an intelligence warrant (human intelligence activities);
  5. Conducting surveillance in a public place;
  6. Obtaining and using publicly available information (open source information);
  7. Making requests for information from other agencies;
  8. Information management;
  9. Making false or misleading representations about being employed by an intelligence and security agency;
  10. Activities covered by the exemption from the Land Transport (Road User) Rule 2004; and
  11. Cooperation with overseas public authorities, including providing advice and assistance to and sharing intelligence with overseas public authorities.

[HYPERLINK TO EACH]

11. MPSs take effect from the date of signing and continue in effect for three years. The Minister responsible for GCSB and NZSIS may, amend, revoke or replace any of the MPSs at any time. However, they must consult with the Inspector-General of Intelligence and Security, any other relevant Minister, or any other person the Minister considers appropriate.
12. The Minister can issue further MPSs on other areas if considered necessary or desirable.

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982



## *Ministerial Policy Statement*

# Cooperating with overseas public authorities

[\[Link to landing page on purpose of MPSs\]](#)

### Summary

It is important for New Zealand's security for GCSB and NZSIS to cooperate with overseas public authorities, including overseas intelligence agencies.

This Ministerial Policy Statement (MPS) provides guidance for GCSB and NZSIS in relation to cooperation with overseas public authorities. In making decisions related to foreign cooperation, employees must have regard to the following principles: respect for human rights, necessity, reasonableness and proportionality, protections for New Zealanders, information management and oversight. This MPS also specifies additional matters to be included in internal policy and procedures.

### Definitions

**Cooperation** means to work together, and includes sharing intelligence and providing/receiving services, advice or assistance (including training, methodology and technology). This may be reciprocated or unreciprocated.

**Overseas public authority** means a foreign person or body that performs or exercises any public function, duty, or power conferred on that person or body by or under law.

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

### This MPS provides guidance on overseas cooperation

1. New Zealand has a robust legislative framework to govern the activities of GCSB and NZSIS, including activities that involve cooperation with overseas public authorities. The Act includes obligations for GCSB and NZSIS to act in accordance with New Zealand law and all human rights obligations recognised by New Zealand law,<sup>2</sup> independently and impartially, with integrity and professionalism and in a manner that facilitates effective oversight.

---

<sup>2</sup> Sections 10(3), 12(7), 17(a) and 18(b).

2. Cooperation with foreign partners can sometimes pose a risk of acting unlawfully with both domestic legal obligations and international obligations, including a risk that New Zealand could become complicit in some forms of unlawful conduct by another country.<sup>3</sup> When undertaking overseas cooperation there are also a range of policy, human rights and reputational risks which need to be considered and managed. Consistent with New Zealand's respect for, and promotion of human rights, this MPS therefore provides policy guidance to, and sets expectations on, GCSB and NZSIS that extend beyond their legal obligations.

### **Scope of this MPS**

3. This MPS applies to GCSB and NZSIS when cooperating with an overseas public authority (whether individually, jointly or with other government agencies). Cooperation may occur in relation to the performance of any of the functions of GCSB and NZSIS in sections 10 to 15 of the Act.
4. Cooperation must be lawful to be within scope of this MPS. Before and during foreign cooperation, GCSB and NZSIS must ensure their actions are consistent with their legal obligations. If in doubt, legal advice must be sought. Failure to act in accordance with New Zealand law could lead to possible criminal responsibility for employees of GCSB and NZSIS.

### **Context**

#### ***Ministerial authorisation to cooperate***

---

5. GCSB and NZSIS must obtain Ministerial authorisation where foreign cooperation involves the provision of intelligence, analysis or threat reporting.<sup>4</sup> Ministerial authorisation can be sought on a case-by-case basis, for example to provide specific intelligence during a conference or event (such as APEC). Alternatively, Ministerial authorisation can be sought on a standing basis to provide intelligence to a range of overseas public authorities on an on-going basis.
6. Standing authorisations must be reviewed regularly to ensure that cooperation undertaken under the authorisation remains consistent with the principles in this MPS. In particular, if there are increased risks for ongoing cooperation either from changes to the domestic law, policy or practice of the overseas public authority subject to a standing authorisation, or from evidence they have carried out a significant breach of human rights, the standing authorisation must be reviewed by the responsible Minister on advice by GCSB and NZSIS.

---

<sup>2</sup> Complicity is a legal term which recognises that while a state did not carry out the wrongful act, if it knowingly aided or assisted another state to commit that wrongful act, it may be liable by law.

<sup>4</sup>By contrast, GCSB and NZSIS may provide protective security services to any public authority in New Zealand or overseas without requiring Ministerial authorisation (in accordance with section 11(1)(a) of the Act).

UNCLASSIFIED

7. GCSB and NZSIS must ensure sufficient information regarding the human rights practices of the overseas public authority is provided to the Minister to support decision-making. Guidance on this is contained within Appendix One.

***New Zealand's intelligence and security relationships***

8. New Zealand gains significant value from cooperating with overseas public authorities, particularly within the current climate of global and transnational threats. Close and reliable intelligence relationships help GCSB and NZSIS prioritise and focus their resources on the areas most important to New Zealand, while having access to a much greater pool of information, skills and technology that would not otherwise be available to New Zealand.
9. For example, an overseas partner may have specific linguistic or technical capabilities that GCSB and NZSIS need in order to obtain or assess intelligence relevant to New Zealand's security and intelligence priorities. Similarly, GCSB or NZSIS may provide intelligence to an overseas public authority to alert them to a potential threat to their security, which helps contribute to international security and New Zealand's overall international relations with that country.
10. In the context of protective security services, advice and assistance, GCSB or NZSIS may provide technology or expertise to an overseas public authority to develop, implement or improve upon their protective security arrangements. For example, providing expertise on conducting a security vetting assessment, information security systems or detecting and protecting against cybersecurity threats. Such cooperation helps overseas authorities store and protect New Zealand Government information and contributes to the recipient's national security and the security of their region.
11. The closest relationships GCSB and NZSIS have with overseas public authorities are those with equivalent agencies from Australia, Canada, the United Kingdom and the United States (often referred to as the "Five Eyes" partners). The relationships between Five Eyes partners are long-running, reciprocal, cover a wide range of topics, and involve a high degree of mutual trust, honesty and respect. The relationships provide New Zealand with knowledge and capability far beyond what we can afford on our own. These relationships work effectively due to the shared values and histories of the five countries and the strong relations between the governments of those countries. The depth of the Five Eyes relationship means that disparities in size, power and influence do not prevent any member from acting in the best interests of their own government, and members expect to be able to disagree on specific matters without damaging the broader relationship.
12. The GCSB and NZSIS may cooperate with overseas public authorities from countries beyond the Five Eyes. This cooperation may occur on an ongoing, relatively informal, or one-off basis. The reasons for cooperating with such authorities vary widely and may occur while performing any of the agencies' functions and as part of contributing to their objectives. Examples include – providing support to a major event such as APEC or the Olympic Games, or helping implement a Protective Security framework with an overseas public authority.

***International and domestic obligations***

13. New Zealand's core human rights obligations are detailed at Appendix Two. These include the right to life, the right not to be subjected to torture, the right not to be subjected to cruel, inhuman or degrading treatment or punishment, and the right to liberty and security of the person. New Zealand is also subject to other international obligations. These can be from a range of sources, including customary law obligations or binding United Nations resolutions. These obligations can range in nature from requiring action, prohibiting conduct or recognising rights.
14. The New Zealand Government has a long-standing and strong opposition to the use of torture, cruel, inhuman or degrading treatment or punishment in all cases and under all circumstances, including in response to threats to national security. The prohibition of torture is non-derogable –it can never be violated by states under any circumstances. New Zealand is opposed to the use of 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>5</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>6</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-

---

<sup>5</sup> Under the Second Optional Protocol to the International Covenant on Civil and Political Rights aiming at the abolition of the death penalty.

<sup>6</sup> See s27(2)(ca) Mutual Assistance in Criminal Matters Act and s30(3) of the Extradition Act 1999.

## UNCLASSIFIED

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 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 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

## UNCLASSIFIED

intelligence received, including unsolicited intelligence,<sup>7</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.
  - 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***

---

<sup>7</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

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.

### ***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>8</sup>
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

---

<sup>8</sup> This includes the Public Service Act 2020 and the Health and Safety at Work Act 2015.

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>9</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:

- 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.

---

<sup>9</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.

**Duration of ministerial policy statement**

39. This MPS will take effect from XX for a period of three years. The Minister responsible for the GCSB and NZSIS may, at any time, amend, revoke or replace the MPS.

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

**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.

UNCLASSIFIED

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

## 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

# 2017 VERSION OF MINISTERIAL POLICY STATEMENT: COOPERATING WITH OVERSEAS PUBLIC AUTHORITIES

### Summary

It is important for New Zealand's security for the Government Communications Security Bureau (GCSB) and New Zealand Security Intelligence Service (NZSIS) to cooperate with overseas public authorities, including overseas intelligence agencies.

This ministerial policy statement (MPS) provides guidance for GCSB and NZSIS in relation to all forms of cooperation with overseas public authorities. In making decisions related to foreign cooperation, employees must have regard to the following principles: legality, human rights obligations, necessity, reasonableness and proportionality, protections for New Zealanders, information management and oversight. This MPS also specifies certain additional matters to be included in internal policy and procedures.

### Definitions

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

*Cooperation* means any form of interaction, whether reciprocal or not, with an overseas public authority, including but not limited to training, advice, assistance, and sharing of information, intelligence, analysis, methods and technology.

*GCSB* means the Government Communications Security Bureau.

*NZSIS* means the New Zealand Security Intelligence Service.

*Overseas public authority* means a foreign person or body that performs or exercises any public function, duty, or power conferred on that person or body by or under law.

*Personal information* means information about an identifiable individual.

### Purpose

1. This MPS is issued by the Minister Responsible for the GCSB and the Minister in Charge of the NZSIS pursuant to section 207(1) of the Act.
2. The purpose of the MPS is to provide guidance to GCSB and NZSIS on the conduct of activities that involve cooperation with overseas public authorities. 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 her 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). A copy of this MPS will also be provided to the Intelligence and Security Committee of Parliament.
4. Every employee making decisions or taking any action related to cooperating with an overseas public authority 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 cooperating with an overseas public authority, which includes providing advice and assistance to an overseas public authority and sharing intelligence with an overseas public authority. These activities may occur in relation to any of the functions of GCSB and NZSIS as specified or allowed for in sections 10 to 15 of the Act.
6. For the purposes of this MPS a broad interpretation of cooperation applies, in that specific activities may or may not be reciprocal, but will in some way involve GCSB or NZSIS interaction with an overseas public authority (also referred to as a foreign partner). To this end, it includes the provision of services, advice, assistance and intelligence which is not reciprocated, as well as reciprocally sharing intelligence, acting cooperatively on a project, or providing and receiving services, advice, and assistance. Cooperation may include an overall cooperative relationship between GCSB or NZSIS and an overseas public authority, interactions between employees of GCSB or NZSIS and the overseas public authority, or specific activities that occur as part of cooperation with a foreign partner.
7. GCSB and NZSIS may only request overseas public authorities to carry out activities that, if carried out by GCSB or NZSIS without an authorisation would be unlawful, in accordance with an authorisation issued under part 4 of the Act. In addition, the Directors-General of GCSB and NZSIS may request those authorities (or their personnel) to assist GCSB or NZSIS with giving effect to an authorisation (see section 51(1)). The carrying out of these types of authorised activities must be conducted consistently with the Act and the terms of the relevant authorisation, including any restrictions or conditions set out in the authorisation. This MPS does not apply to requests for assistance and activities which are carried out under an authorisation issued under part 4 of the Act.
8. The primary purpose of this MPS is to provide guidance on determining which overseas public authorities GCSB and NZSIS should engage with, and how that engagement should be regulated, including guidance on the types of activities that are appropriate to undertake with those parties. To the extent that it arises through cooperation with an overseas public authority, the MPS also addresses issues associated with the operational use of intelligence gained from a foreign partner.

### 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;
  - b) The provision of protective security services, advice and assistance;
  - c) Cooperation with other public authorities to facilitate their functions; and
  - d) Cooperation with other entities to respond to imminent threat.

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.

*New Zealand's intelligence and security relationships*

12. The mandate provided by the agencies' objectives and functions is a New Zealand-centric one. Foreign cooperation is based on furthering New Zealand's interests and fulfilling any international obligations New Zealand has.
13. GCSB and NZSIS may cooperate with overseas public authorities in fulfilling any of GCSB's and NZSIS's functions. New Zealand gains significant value from international intelligence sharing and cooperation arrangements, particularly within the current climate of global and transnational threats. Through foreign intelligence partnerships and other cooperation, GCSB and NZSIS are able to draw on a much greater pool of information, skills and technology than would otherwise be available to them. Close and reliable relationships with overseas public authorities help GCSB and NZSIS to prioritise and focus their limited resources on the areas most important to New Zealand, while having access to resources that would not normally be available.
14. For example, a foreign partner may have access to information that requires specific linguistic, ethnic or cultural backgrounds to collect and analyse which New Zealand does not possess. As part of their intelligence collection and analysis function, GCSB and NZSIS may seek to obtain that intelligence. Similarly, GCSB or NZSIS might provide intelligence to an overseas public authority so that authority can take action to address a threat to New Zealand's national security (such as a threat to New Zealanders overseas), or to contribute to New Zealand's international relations with the partner country.
15. In the context of protective security services, advice and assistance, GCSB or NZSIS might provide technology or expertise to an overseas public authority (which might include seconding staff) to support that authority with its own protective security requirements, such as systems for vetting security cleared personnel, or detecting cybersecurity threats. This advice and assistance could contribute to New Zealand's national security by mitigating common threats and developing international relations with the partner countries, and contribute to New Zealand's economic well-being by reducing risks to New Zealand companies operating overseas.
16. The closest relationships that GCSB and NZSIS have with overseas public authorities are those with equivalent agencies from Australia, Canada, the United Kingdom and the United States (often referred to as the "Five Eyes" partners). The relationships between Five Eyes partners are long-running, reciprocal, cover a wide range of topics, and involve a high degree of mutual trust, honesty and respect. The relationships provide New Zealand with knowledge and capability far beyond what we can afford on our own.
17. These relationships work effectively due to the shared values and histories of the five countries and the strong relations between the governments of those countries in general. The depth of the Five Eyes relationship means that disparities in size, power and influence do not prevent any member from acting in the best interests of their own government, and members expect to be able to disagree on specific matters without damaging the broader relationship.
18. GCSB and NZSIS may also cooperate with overseas public authorities from other countries. This cooperation may occur on a routine or relatively ad hoc basis. The reasons for cooperating with such authorities may vary widely and may occur in the course of performing any of the agencies' functions and as part of contributing to any of their objectives. It is essential to New Zealand's ability to protect its national security,

international relations and economic well-being to share information and intelligence with agencies outside traditional partnerships.

#### *International obligations*

19. New Zealand may be subject to international obligations to cooperate with overseas partners, in order to promote the exchange of information to help improve international responses to threats to global peace and security. For example, United Nations Security Council Resolution 1373 (2001) calls on states to “find ways of intensifying and accelerating the exchange of operational information, especially regarding actions and movements of terrorist persons or networks”. Under this resolution, Member States are required to have in place procedures and mechanisms that encourage exchange of information in accordance with international and domestic law, which includes international human rights obligations.
20. The many positive benefits of New Zealand’s participation in foreign intelligence and security relationships do not override the rights of New Zealanders and the international human rights obligations New Zealand has adopted through their incorporation into domestic law. New Zealand is also subject to other international obligations, including through customary international law and as a member of the United Nations. For example, New Zealand is bound by United National Security Council Resolution 1456 (2003), which requires Member states to “ensure that any measure taken to combat terrorism comply with all their obligations under international law, and should adopt such measures in accordance with international law, in particular international human rights, refugee and humanitarian law”.
21. New Zealand’s core international human rights obligations, including those at customary international law, are detailed at Appendix One. They include the right to life, the right not to be subjected to torture, the right not to be subjected to cruel, inhuman or degrading treatment or punishment, and the right to liberty and security of the person.
22. The New Zealand Government has a long-standing and strong opposition to the use of torture, cruel, inhuman or degrading treatment or punishment (including the death penalty) in all cases and under all circumstances, including in response to threats to national security. New Zealand is committed to actively preventing torture, cruel, inhuman or degrading treatment or punishment, and will not, by act or omission, encourage, aid, or abet such action.

#### *Duty to act with due diligence*

23. Section 17(a) of the Act imposes a general duty on GCSB and NZSIS to act in accordance with New Zealand law and all human rights obligations recognised by New Zealand law. Sections 10(3) and 12(7) also explicitly impose an obligation on the responsible Minister to be satisfied the agencies will be acting consistently with such law when authorising the sharing of intelligence, analysis and threat reporting with foreign partners. Compliance with this obligation necessitates a practice of due diligence by the Directors-General of GCSB and NZSIS in relation to cooperation with overseas public authorities. The guidance in this MPS provides a framework for exercising that due diligence when determining whether it will be appropriate to engage with a particular overseas public authority, and when determining that the proposed activities are consistent with the law – particularly with respect to ensuring that GCSB and NZSIS do not become complicit in human rights abuses.
24. The Directors-General have a duty to take steps as are reasonable in the circumstances of each particular situation to identify risks of human rights being breached by partner countries and international actors. To ensure that agencies are not associated (either

directly or indirectly) with activities that may be unlawful or improper, as a result of cooperation with an overseas public authority, it is expected that GCSB and NZSIS will establish an awareness of and regularly monitor the human rights practices of any overseas public authorities with which the agencies cooperate. The agencies are also expected to further enquire when there is an indication that human rights breaches might occur in a situation, and decline or stop cooperating with the overseas public authority where a real or substantial risk of breach of human rights obligations (such as the prohibition of torture) is identified.

25. Failure to act in accordance with the provisions of the Act and this MPS could lead to possible criminal responsibility for employees of GCSB and NZSIS. For example, Section 3 of the Crimes of Torture Act 1989, which applies to activities conducted within or outside New Zealand, makes it a crime for a public official or anyone acting in an official capacity to attempt or to commit an act of torture, to act or omit to act in a way that aids any person to commit an act of torture, to abet any person in the commission of an act of torture, or to incite, counsel, procure or conspire with any person to commit an act of torture, and to be an accessory after the fact to an act of torture.

*Unsolicited intelligence*

26. The absolute prohibition in international law (and which is incorporated in New Zealand law) on the use of information gained through torture for evidentiary purposes arises from the need to remove any incentives to torture and recognises that such information is inherently unreliable. This obligation is non-derogable – it cannot be violated by states under any circumstances.

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

27. There may be exceptional circumstances where unsolicited intelligence is received by GCSB or NZSIS that indicates a credible national security threat to New Zealand or risk to New Zealanders that has been, or is suspected to have been, obtained through human rights abuses committed by another party.
28. GCSB and NZSIS do not have an enforcement function in relation to measures to protect national security. If intelligence is received that indicates a credible risk to the safety of New Zealanders that requires action to be taken to protect lives and property, GCSB and NZSIS must provide that information to the relevant enforcement agency. The information will not be used for evidentiary purposes in legal proceedings.

### **Principles**

29. The following principles constitute a framework for good decision-making and must be taken into account by GCSB and NZSIS when cooperating with overseas public authorities in the performance of one or more of the agencies' functions. All forms of cooperation with overseas public authorities, at all levels, should be subject to ongoing review as to whether it continues to be consistent with these principles.

#### *Legality*

30. GCSB and NZSIS must ensure that cooperation with overseas public authorities is conducted in accordance with New Zealand law and all human rights obligations recognised by New Zealand law. GCSB and NZSIS should also have regard to New Zealand's human rights obligations at international law, including customary international law (see Appendix One).
31. For all forms of cooperation with overseas public authorities, GCSB and NZSIS must have internal policies in place that ensure the agencies act in accordance with New Zealand law and all human rights obligations recognised by New Zealand law; and must have procedures in place to ensure those policies have been adhered to. Where appropriate, legal advice should be sought.
32. Where Ministerial approval for cooperation is required, GCSB and NZSIS have a positive obligation to provide sufficient information regarding the legality of cooperation with overseas public authorities to the Minister, in order for the Minister to determine whether the requirements under sections 10(3) and 12(7) of the Act are met.
33. Where there may be uncertainty or cause for concern as to whether cooperation with an overseas public authority is lawful, specific information detailing the nature of the cooperation and the factors that gave rise to that uncertainty or concern (such as examples of previous actions by the foreign partner, external reports, or advice from the Ministry of Foreign Affairs and Trade) should be provided to the responsible Minister (in the case of Ministerial approvals) to assist decision-making, or to the Director-General (in the case of internal approvals).
34. Where necessary, the Ministry of Justice should be consulted on New Zealand's human rights law and information sought from the Ministry of Foreign Affairs and Trade regarding New Zealand's international human rights obligations and the adherence of other countries to these obligations.

#### *Human rights obligations*

35. GCSB and NZSIS must not undertake any activity in cooperation with an overseas public authority, including receiving or sharing any intelligence, where GCSB or NZSIS knows or assesses that there is a real risk that the activity will lead to or has been obtained as a result of human rights breaches in any country, against any person(s). In these

circumstances, the continued receipt or sharing of intelligence should cease, subject to a reassessment in accordance with legal obligations, the principles in this MPS and relevant policies.

36. This provides a duty to apply due diligence: GCSB and NZSIS are to assess the likelihood of human rights breaches occurring (or having occurred) in connection with any sharing of intelligence or cooperation by the agencies with an overseas public authority, including in any subsequent actions taken by that public authority as a result of the cooperation or sharing of intelligence.
37. To avoid any complicity in human rights breaches by an overseas public authority, when assessing this likelihood, GCSB and NZSIS must take into account factors such as:
  - 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;
  - whether the country has ratified relevant international human rights treaties, including any reservations that may have been made;
  - whether the country has mechanisms for independently investigating breaches of human rights;
  - whether the country has an independent judiciary with jurisdiction to hear cases relating to breaches of human rights;
  - whether the country has an established history of compliance with human rights obligations;
  - whether the country has an established history of investigating and prosecuting human rights breaches; and
  - 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.
38. When authorising the provision of intelligence and analysis, or the provision of threat reports produced from the provision of information assurance and cybersecurity activities, to an overseas public authority, the responsible Minister must be satisfied that GCSB and NZSIS will be acting in accordance with New Zealand domestic law, including all human rights obligations recognised by New Zealand law.
39. The Minister must be satisfied of this on the basis of information provided to him or her by GCSB or NZSIS about the particular proposal to share intelligence, analysis or threat reporting. The Minister's authorisation may be made on a case-by-case basis or may take the form of a broader standing authorisation, for example to share specific categories of intelligence, analysis or threat reporting with certain overseas public authorities, or to share the full range of intelligence, analysis or threat reporting within an established intelligence and security relationship with a foreign country, groups of countries or overseas public authority.
40. A request to share intelligence, analysis and threat reporting with a foreign partner, whether on a case-by-case basis, or within the context of a broader standing authorisation, must include information about the specific proposal and must include an assessment of the human rights practices of the foreign partner, or describe the process by which the agencies will make that assessment. The assessment must be based on:
  - the human rights record of the country (as reflected in the considerations at paragraph 37 above)

- any particular risks to human rights associated with the proposed cooperation and how likely it is that breaches could occur; and
  - factors that mitigate the likelihood of human rights breaches occurring. Such factors might include the existence and effectiveness of mechanisms for monitoring or reviewing compliance with human rights obligations, 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 how likely the foreign partner is to comply with caveats associated with cooperation or use of information.
41. The decision to authorise the sharing of intelligence, analysis or threat reporting with a foreign partner, whether made by the Minister on a case-by-case basis or by the agencies within a broader standing authorisation, must also consider:
- all applicable legal obligations under New Zealand and international law, and any relevant international commitments New Zealand may have; and
  - the purpose of the intelligence sharing, including how it contributes to GCSB's and NZSIS's statutory objectives to contribute to the protection of New Zealand's national security, the international relations and well-being of New Zealand, and the economic well-being of New Zealand.
42. The responsible Minister may issue standing authorisations for GCSB or NZSIS to share specific classes of intelligence, analysis and threat reporting with certain overseas public authorities, or to share intelligence, analysis and threat reporting with a specific overseas public authority or with a particular country or group of countries. When issuing a standing authorisation, the Minister must be satisfied on the basis of an assessment which considers the same factors in paragraphs 40 and 41 above. Standing authorisations may specify conditions, limits or exclusions that apply in respect of the sharing of intelligence, analysis and threat reporting under the authorisation. The Minister will specify thresholds of risk at which decisions made under a standing authorisation must be referred back to the responsible Minister.
43. The existence of a standing authorisation does not excuse GCSB and NZSIS of the obligation to undertake ongoing monitoring to ensure that cooperation undertaken under the authorisation remains consistent with the framework in this MPS. In particular, the agencies must conduct a risk assessment of human rights breaches occurring if there is any reason to believe a specific instance of cooperation might lead to such an infringement. Further, if there is evidence that a human rights breach has occurred, or there are changes to domestic policy or practice in any country subject to a standing authorisation that may increase the likelihood of violations of human rights, the standing authorisation must be reviewed by the responsible Minister.
44. Where Ministerial authorisation for cooperation is not required, GCSB and NZSIS must have processes that require internal authorisation to cooperate with an overseas public authority to be granted by appropriately senior staff, according to an assessment of the risk of human rights breaches connected with that cooperation. Where there is a reasonable basis for concern about a country's human rights record or that the cooperation in question might involve complicity in breaches of human rights, GCSB and NZSIS must seek authorisation from the responsible Minister before undertaking any cooperation. GCSB and NZSIS must provide the Minister with an assessment that addresses the factors outlined at paragraphs 40 and 41.
45. If GCSB or NZSIS become aware that their cooperation with an overseas public authority means GCSB or NZSIS may have been complicit in human rights breaches the agency must immediately suspend cooperation with that authority (and any others related to it) and

notify the responsible Minister and the Inspector-General of Intelligence and Security, and if necessary, the Solicitor-General. An internal review to determine whether agency policies and procedures were correctly applied in respect of the cooperation must also be conducted by the relevant agency.

46. In the event GCSB or NZSIS receives unsolicited information indicating a credible national security risk to New Zealand or risk to the safety of New Zealanders, but that has been, or is suspected to have been, obtained through human rights abuses committed by another party the Directors-General will consider the need to ensure public safety and the protection of life and property in determining whether to pass that information to the relevant enforcement agency. In considering whether to pass on the information for operational purposes, GCSB and NZSIS must be mindful that the reliability of such information may be limited. Where information of this nature is passed on, the responsible Minister and the Inspector-General of Intelligence and Security must be informed as soon as practicable.

#### *Necessity*

47. Cooperation by GCSB or NZSIS with any foreign partner must be for the purpose of protecting New Zealand's national security, the international relations and well-being of New Zealand, and the economic well-being of New Zealand. Specific cooperation with overseas public authorities should only occur for purposes necessary to support the agencies to perform their statutory functions. This may include building the capacity of GCSB or NZSIS to perform a particular statutory function, or for establishing or maintaining an international relationship that will support GCSB or NZSIS to perform their statutory functions.

#### *Reasonableness and proportionality*

48. The impact of 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.
49. Relevant factors in determining the reasonableness and proportionality of cooperation with an overseas public authority include:
- having a clear understanding of the nature and purpose of the specific activities and any subsequent actions that are likely to result;
  - having a clear understanding of the nature and purpose of the intelligence and security relationship with the particular overseas public authority;
  - being aware of the status of the bilateral relationship with the country as a whole (especially any issues or areas of sensitivity between New Zealand and the partner country that could have a bearing on the proposed activities);
  - any limitations or restrictions on activity that either party has; and
  - any protections that may be in place in relation to the activity or to intelligence provided or received.
50. For example, when New Zealand is seeking assistance or intelligence or information from partners, GCSB or NZSIS should be clear as to why they seek the assistance or intelligence or information from the partner country, and about the expectations of the New Zealand Government that no human rights breaches occur in the provision of that assistance or in the collection or provision of the intelligence or information.



51. Where New Zealand is asked to provide assistance, intelligence or information by overseas partners, GCSB or NZSIS should be as informed as is possible about the particular situation. This should include being aware of the purpose and value of the proposed activity and that there is sufficient evidence, not based on human rights breaches, of the need for the activity.
52. For example, when sharing intelligence, this would include consideration of whether this was reciprocal sharing of intelligence on a routine and systematic basis, as part of a wider intelligence relationship; regular sharing of intelligence but on a case-by-case basis; responding to one-off ad hoc (and potentially urgent) requests for intelligence; or pro-active ad hoc sharing by the agencies to mitigate a risk to a third country.

#### *Protections for New Zealanders*

53. When cooperating with overseas public authorities, GCSB and NZSIS must continue to apply the same protections for New Zealand citizens and permanent residents 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.
54. Where cooperation with an overseas public authority involves the sharing of intelligence or personal information relating to New Zealanders, GCSB and NZSIS must have particular regard to the privacy interests of the New Zealanders when determining whether to disclose that personal information to overseas partners, or when requesting such information from overseas partners. This includes adherence to the [information privacy principles](#) contained in Part 2 of the Privacy Act 1993 as they apply to GCSB and NZSIS. GCSB and NZSIS must be satisfied that the overseas public authority has adequate protections in place for the use and storage of New Zealanders' information, including adequate protections against further sharing with third parties without express consent from GCSB or NZSIS.

#### *Information management*

55. GCSB and NZSIS will take steps to ensure that information obtained by GCSB and NZSIS and subsequently shared with overseas public authorities is managed in accordance with all information management requirements, standards and guidelines that relate to that information (such as the New Zealand Protective Security Requirements, New Zealand Government Security Classification System, and New Zealand Information Security Manual), and any other obligations as addressed in the MPS on *Management of information obtained by GCSB and NZSIS*.
56. GCSB and NZSIS are to specify the protection, storage and use (including restrictions on the passing on of that information to any third parties) requirements that are to be adhered to in respect of any information, including personal information about New Zealanders, shared with an overseas public authority. Those requirements will be consistent with the principles in this MPS and the MPS on *Management of information obtained by GCSB and NZSIS*. It is recognised that the overseas public authority may be required to adhere its own national requirements when managing received information and this may conflict with conditions imposed by GCSB or NZSIS. GCSB and NZSIS should seek to be consulted regarding any national requirements of an overseas partner that may lead to shared information being used in a manner that conflicts with restrictions that would apply in New Zealand.

## Oversight

57. GCSB and NZSIS must carry out all cooperation with overseas public authorities in a manner that facilitates effective accountability, transparency and oversight. This includes the use of clear authorisation procedures, the keeping of appropriate records, maintaining up-to-date internal policies and procedures and guidance for staff, and reporting to the responsible Minister on the nature and outcomes of cooperation with overseas public authorities. 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**

58. 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. Those policies and procedures must also address the following additional matters:

#### **Human rights policy**

GCSB and NZSIS must have a policy setting out the factors that must be considered when assessing whether a real risk of human rights breaches may exist in connection with cooperation with overseas public authorities. This policy must also include what specific information is required to be provided to the responsible Minister before authorisation (either on a case-by-case basis or in the form of a broader standing authorisation) is given to share intelligence or analysis to an overseas public authority.

This policy is important to ensure that employees do not inadvertently place themselves or the New Zealand Government at legal risk by their action or inaction.

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

Foreign policy objectives should be considered in the development and framing of cooperation arrangements with foreign partners. The Ministry of Foreign Affairs and Trade is to be consulted on any proposal to enter into an arrangement with a foreign jurisdiction or international organisation.

GCSB and NZSIS should also seek information from, and have regard to any information provided by, the Ministry of Foreign Affairs and Trade on the status of the bilateral relationship with a country, and when weighing up factors related to a country's ratification of international human rights treaties and the human rights record of a particular country.

#### **Written basis for new formal arrangements**

All new bilateral or multilateral arrangements relating to cooperation and intelligence sharing with a foreign jurisdiction or overseas public authority must be referred to the Intelligence and Security Committee of Parliament for noting. Such arrangements should be recorded in writing.

GCSB and NZSIS must formulate standard terms for ad hoc cooperation and intelligence sharing, which are to be recorded in an internal policy. These terms are to establish consistent principles, standards and practices that will be applied to ad hoc cooperation and intelligence sharing activities to ensure that GCSB and NZSIS complies with New Zealand law and all human rights obligations recognised by New Zealand law. Those terms should be consistent with this MPS. These terms must be forwarded in draft to the Inspector-General of Intelligence and Security for comment and the final version referred to the Intelligence and Security Committee of Parliament for noting.

#### **Training**

All employees of GCSB and NZSIS must be provided training on all relevant law, policies and procedures in relation to the agencies' human rights obligations. This training should be provided for all existing employees and for new employees at induction, and whenever there are changes or updates to the policies and procedures, to ensure that at all times employees are aware of their obligations.

## Compliance with 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.

## Health and safety

All cooperation with overseas public authorities must be undertaken consistently with GCSB's and NZSIS's obligations under the Health and Safety at Work Act 2015.

## Authorisation procedures

59. Within the context of this MPS, the responsible Minister must authorise the following:

- The provision of any intelligence collected and any analysis of that intelligence to an overseas public authority
- The provision of threat reports produced as a result of information assurance and cybersecurity activities to an overseas public authority

60. In determining whether to authorise the sharing of intelligence, analysis and threat reporting to an overseas public authority, the Minister must be satisfied that GCSB and NZSIS will be acting in accordance with New Zealand law including all human rights obligations recognised by New Zealand law.

61. The Minister will authorise the sharing of intelligence, analysis or threat reporting with a foreign partner on the basis of information provided to him or her by GCSB and NZSIS. This authorisation may be on a case-by-case basis or in the form of a broader standing authorisation. All requests for authorisation to share intelligence, analysis and threat reporting must include an assessment that addresses all factors listed in paragraphs 40 and 41 of this MPS, or describe how the agencies will make that assessment.

62. GCSB and NZSIS may seek a standing authorisation from the Minister that covers the sharing of specific classes of intelligence, analysis and threat reporting with certain overseas public authorities, or to share intelligence, analysis and threat reporting with a specific overseas public authority or with a particular country or group of countries. A request for a standing authorisation must include an assessment which considers the factors outlined in paragraphs 40 and 41 of this MPS, or describe how the agencies will make that assessment.

63. The Minister may specify conditions, limits or exclusions that are to apply in respect of the sharing of intelligence, analysis and threat reporting with an overseas public authority or country under a standing authorisation. The Minister will specify thresholds of risk at which decisions made under a standing authorisation must be referred back to the Minister. Standing authorisations must be reviewed when this MPS is amended, revoked or replaced, and if a human rights breach occurs or there are changes to domestic policy or practice in the country that may increase the likelihood of violations of human rights.

64. Where Ministerial authorisation for cooperation is not required, there must be clear levels of decision-making for each type of activity that may involve foreign cooperation, which must be documented. GCSB and NZSIS must have in place approval levels that are proportionate to the operational, reputational, legal and health and safety risks in cooperation with overseas public authorities: the greater the risk, the more senior the level of approval required. An assessment of the risk of human rights breaches connected with the foreign cooperation must be carried out, that includes the considerations outlined at paragraphs 40 and 41 of this MPS. Approval levels will include seeking authorisation from the Minister at agreed levels of risk, in particular where there is a reasonable basis for concern about a country's human rights record or that the cooperation in question might involve complicity in breaches of human rights.

65. The Directors-General of GCSB and NZSIS may authorise the passing of unsolicited intelligence indicating a credible national security risk to New Zealand or risk to the safety of New Zealanders that has been, or is suspected to have been, obtained through human right abuses committed by another party, to an enforcement agency. The Directors-General must consider the need to ensure public safety and the protection of life and property, and must be mindful that the reliability of such information is likely to be limited. If such information is passed on to an enforcement agency the responsible Minister and Inspector-General of Intelligence and Security must be informed as soon as practicable.

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

### Duration of ministerial policy statement

66. This MPS will take effect from 28 September 2017 for a period of three years. The Minister who issued an MPS may, at any time, amend, revoke or replace the MPS.
67. At the time of issue of this MPS, the Inspector-General of Intelligence and Security is undertaking an Inquiry into possible New Zealand engagement with Central Intelligence Agency (CIA) detention and interrogation, 2001-2009, and current intelligence cooperation safeguards. When completed, the conclusions from that inquiry may give cause for the issuing Minister to review and reissue this MPS.

---

Ministerial Policy Statement issued by:



Hon Christopher Finlayson  
Minister responsible for the Government Communications Security Service  
Minister in charge of the New Zealand Security Intelligence Service

September 2017

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

# Appendix One:

## 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 1993
- 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, 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.

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

# ATTACHMENT C

## Letter to Hon Nanaia Mahuta, Minister of Foreign Affairs

Hon Nanaia Mahuta  
Minister of Foreign Affairs  
Parliament Buildings

Dear Minister Mahuta

### **Consultation on Ministerial Policy Statement – Cooperating with Overseas Public Authorities**

I enclose for your comment a draft of the revised Ministerial Policy Statement (MPS) regarding GCSB and NZSIS cooperation with overseas public authorities.

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 Foreign Affairs.

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

Given your portfolio responsibilities in supporting New Zealand's international agreements, commitments and obligations, and your role in overseeing the development of the detention policy as part of the government response to Operation Burnham, I would welcome any insights that you may have on overseas cooperation. Officials from the Department of the Prime Minister and Cabinet have liaised with officials from the Ministry of Foreign Affairs and Trade 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 D

## Letter to Hon Poto Williams, Minister of Police

Hon Poto Williams  
Minister of Police  
Parliament Buildings

Dear Minister Williams

### **Consultation on Ministerial Policy Statement – Cooperating with Overseas Public Authorities**

I enclose for your comment a draft of the revised Ministerial Policy Statement (MPS) regarding GCSB and NZSIS cooperation with overseas public authorities.

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 Police also undertake similar cooperation with overseas authorities, I would welcome insights that you may have on the guidance in this MPS or ways that we might better align our respective portfolios' policies on foreign cooperation. Officials from the Department of the Prime Minister and Cabinet have liaised with officials from the 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 E

### Letter to Hon Kris Faafoi, Minister of Justice, Minister of Immigration

Hon Kris Faafoi  
Minister of Justice and Minister of Immigration  
Parliament Buildings

Dear Minister Faafoi

#### **Consultation on Ministerial Policy Statement – Cooperating with Overseas Public Authorities**

I enclose for your comment a draft of the revised Ministerial Policy Statement (MPS) regarding GCSB and NZSIS cooperation with overseas public authorities.

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 Justice.

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

Noting your portfolio responsibilities in supporting New Zealand's human rights commitments and obligations, I would welcome insights that you may have on overseas cooperation or the guidance in this MPS. 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. You may also have comments from your Immigration portfolio, given the intelligence functions of Immigration New Zealand.

Yours sincerely

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

# ATTACHMENT F

## Letter to Hon Peeni Henare, Minister of Defence

Hon Peeni Henare  
Minister of Defence  
Parliament Buildings

Dear Minister Henare

### **Consultation on Ministerial Policy Statement – Cooperating with Overseas Public Authorities**

I enclose for your comment a draft of the revised Ministerial Policy Statement (MPS) regarding GCSB and NZSIS cooperation with overseas public authorities.

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 Defence.

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

Given the New Zealand Defence Force also undertakes intelligence and capacity-building cooperation with overseas authorities, I would welcome any insights that you may have on overseas cooperation, and ways that we might better align our respective portfolios' policies on foreign cooperation. You may also have comments in relation to any issues being considered as part of the government's response to the Operation Burnham Inquiry. Officials from the Department of the Prime Minister and Cabinet have liaised with officials from the Ministry of Defence and the New Zealand Defence Force 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 Meka Whaitiri, Minister of Customs

Hon Meka Whaitiri  
Minister of Customs  
Parliament Buildings

Dear Minister Whaitiri

### **Consultation on Ministerial Policy Statement – Cooperating with Overseas Public Authorities**

I enclose for your comment a draft of the revised Ministerial Policy Statement (MPS) regarding GCSB and NZSIS cooperation with overseas public authorities.

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 Customs.

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

Given the New Zealand Customs Service also undertake similar cooperation with overseas authorities, I would welcome any insights that you may have on overseas cooperation or ways that we might better align our respective portfolios' policies on foreign cooperation. Officials from the Department of the Prime Minister and Cabinet have liaised with officials from NZ Customs 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

## MINISTERIAL POLICY STATEMENT: COOPERATING WITH OVERSEAS PUBLIC AUTHORITIES – APPROVAL TO REISSUE

To Minister Responsible for the GCSB and NZSIS (Hon Andrew Little)			
Date	12/03/2021	Priority	Routine
Deadline	26/03/2021	Briefing Number	2021NSP/066


### Purpose

This briefing seeks your approval to reissue the revised Ministerial Policy Statement (MPS): Cooperating with overseas public authorities. The revised MPS and draft letters to the Director-General of Security and the Director-General of the Government Communications Security Bureau, attaching the MPS and setting out your expectations in relation to implementing the revised MPS, are appended for your signature.

### Recommendations

1. **Note** that all consultation required under the Intelligence and Security Act 2027 has been undertaken on the revised MPS: Cooperating with overseas public authorities;
2. **Agree** not to amend the MPS to incorporate the feedback received from the Minister of Justice, as it would mean the MPS does not align with the Intelligence and Security Act 2017 (see para 5); YES / NO
3. **Sign** the attached letter to the Minister of Justice, notifying him of your decision not to amend the MPS proposed in his feedback; YES / NO
4. **Agree** to reissue the revised MPS: Cooperating with overseas public authorities; YES / NO
5. **Sign** the attached letters to the Director-General of Security and the Director-General of the Government Communications Security Bureau, attaching the revised MPS and setting out your expectations in relation to implementing the revised MPS; YES / NO

6. **Note** that the Directors-General of the intelligence and security agencies are required to make the MPS publicly available on their Internet site as soon as practicable after the MPS is reissued; and
7. **Note** that DPMC will work with your office to ensure the revised MPS is referred to the Intelligence and Security Committee, as required by section 207 (2) of the Intelligence and Security Act 2017.

  
Tony Lynch  
**Deputy Chief Executive**  
National Security Group

---

12.3/2021

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	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

NSP/

# MINISTERIAL POLICY STATEMENT: COOPERATING WITH OVERSEAS PUBLIC AUTHORITIES – APPROVAL TO REISSUE

## Purpose

---

1. This briefing seeks your approval to reissue the revised Ministerial Policy Statement (MPS): Cooperating with overseas public authorities. The revised MPS and draft letters to the Director-General of Security and the Director-General of the Government Communications Security Bureau, attaching the MPS and setting out your expectations in relation to implementing the revised MPS, are appended for your signature.

## Reviewing the MPS: Cooperating with overseas public authorities

---

2. We have completed the review of the MPS: Cooperating with overseas public authorities. We briefed you recently on the main changes to the MPS (2021NSP/030), which include:
  - Removing common content of the MPSs into a cover-sheet that sets out the overarching purpose of the MPSs
  - Clarifying it only applies to lawful activity
  - Including a human rights assessment framework
  - Providing consistency in the threshold that should be applied when assessing when information should not be shared (where there is a real risk of contributing to human rights abuses)
  - Providing criteria the agencies need to take into account when referring a written arrangement to the Intelligence and Security Committee.

## Ministerial consultation on the MPS

---

3. You consulted the following Ministers on the revised MPS, as required under the Intelligence and Security Act 2017 (the Act):
  - Minister of Foreign Affairs
  - Minister of Police
  - Minister of Justice
  - Minister of Immigration
  - Minister of Defence



- Minister of Customs.
4. The Ministers of Immigration, Customs and Defence responded to say they were happy with the revised MPS and were pleased it took their agencies' feedback into account. The Minister of Foreign Affairs and the Minister of Police did not respond.
  5. The Minister of Justice suggested that *'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'*. We considered this feedback, but do not recommend the MPS is amended as a result. This is because:
    - a) The term in the MPS *'all human rights obligations recognised by New Zealand law'* is the wording from the Act. Amending this text would make the MPS inconsistent with the Act;
    - b) The proposed wording suggested by the Minister of Justice 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; and
    - 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. It is not necessary to provide an exhaustive list of obligations in the body of the MPS.
  6. The Ministry of Justice did not raise this feedback during cross-agency consultation. GCSB and NZSIS agree that the MPS should not be amended as a result of the Minister of Justice's feedback.
  7. We therefore recommend you agree to issue the MPS, and to do so without the Minister of Justice's proposed amendment. If you agree, we have attached a letter for you to send to the Minister of Justice notifying him of this.

**You agreed to provide additional guidance on two matters when the MPS is reissued**

---

8. In December 2020 (2021NSP/030), you agreed to provide additional guidance, over and above the MPS itself, to the agencies on two matters:

- s6(a)



- s6(a)



s6(a)



9. Additional guidance on these matters has been set out in the attached letters to the Directors-General. We suggest the letter is copied to the Inspector-General of Intelligence and Security and forwarded to the Intelligence and Security Committee as these matters are relevant to their oversight roles.

## Consultation

---

10. GCSB and NZSIS were consulted on the recommendation resulting from the Ministerial consultation on the MPS and their feedback was incorporated. The agencies were also invited to correct any factual errors in a draft version of this briefing.

## Next steps

---

11. We attach draft letters from you to the Director-General of Security and the Director-General of the Government Communications Security Bureau to confirm you have approved the reissue of this MPS. In addition to the matters above, the letters request that the Directors-General fully implement any changes to internal policies, work programmes and training to implement the revised MPS. This includes revising the Joint Policy Statement on Human Rights Risk Management (JPS). This MPS and the JPS must be referred to the ISC for noting. We will work with your office and the GCSB and NZSIS to ensure this occurs in a timely fashion.
12. If you agree to the revised MPS being reissued, we will arrange for publication on the New Zealand Intelligence Community website on 1 April 2021.
13. We are working towards the other MPSs being ready to be reissued in mid-2021.

Attachments:		
<b>Attachment A:</b>	UNCLASSIFIED	Revised Ministerial Policy Statement: Cooperating with overseas public authorities
<b>Attachment B:</b>	RESTRICTED	Letter to Director-General of Security
<b>Attachment C:</b>	RESTRICTED	Letter to Director-General of Government Communications and Security Bureau
<b>Attachment D:</b>	UNCLASSIFIED	Letter to Hon Kris Faafoi, Minister of Justice

# ATTACHMENT A

Revised ministerial policy statement: Cooperating with overseas public authorities

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982



## *Ministerial Policy Statements*

1. Ministerial Policy Statements (MPSs) are statements issued by the Minister Responsible for the GCSB and NZSIS under section 206 and 207(1) of the Intelligence and Security Act 2017 ('the Act').

### **MPSs provide guidance to GCSB and NZSIS on certain lawful activities**

2. MPSs provide guidance to GCSB and NZSIS (also called 'the agencies') on lawful activities under the Act. They do not act as legal authorisations for these activities but set out the Minister's expectations of how the activities covered by the MPS should be properly carried out and any protections or restrictions in relation to the activity. Activities which are unlawful may only be carried out to the extent that they can be authorised under an intelligence warrant.
3. Every employee making decisions or taking any action in relation to the matters covered by the MPSs must consider and should be able to explain how they had regard to the MPS. This might include an explanation of the consideration of any relevant internal policy or procedures that reflect the MPS. The Directors-General of the GCSB and NZSIS are responsible for ensuring each MPS is reflected in their agency's internal policies and procedures. If any action is taken that is inconsistent with the MPS, employees must be able to explain why that action was taken.

### **They are also considered by the Inspector-General of Intelligence and Security when conducting an inquiry or review**

4. MPSs are relevant to the oversight of the agencies by the Inspector-General of Intelligence and Security in the exercise of their propriety jurisdiction. When conducting an inquiry or review, the Inspector-General of Intelligence and Security must take account of any relevant MPS and the extent to which an agency has complied with it.

### **And they assist in increasing transparency with the New Zealand public**

5. While the primary purpose of the MPSs is to provide guidance to the agencies on their lawful activities, they also provide the public with information on how and why the agencies carry out these activities to help keep New Zealand secure.

### **Each of the activities covered by the MPSs enable the agencies to perform their statutory functions**

6. The Act sets the principal objectives of GCSB and NZSIS, which are to contribute to:
  - The protection of New Zealand's national security;
  - The international relations and well-being of New Zealand; and
  - The economic well-being of New Zealand.
7. The GCSB and NZSIS meet these objectives through the performance of their statutory functions, namely:

UNCLASSIFIED

- Intelligence collection and analysis;
  - Protective security services, advice and assistance;
  - Cooperation with other public authorities to facilitate their functions; and
  - Cooperation with other entities to respond to imminent threat.
8. All collection and analysis of intelligence undertaken by GCSB and NZSIS is in accordance with the New Zealand Government's priorities. These are primarily established through the National Security and Intelligence Priorities (NSIPs) which are set by the Government and reviewed every two years. The NSIPs outline the focus areas for all intelligence and assessment activity across the national security sector, including GCSB and NZSIS.
9. MPSs are an important part of the measures put in place by the Act to ensure these functions are carried out properly.

**Matters covered by the MPSs**

10. The MPSs cover areas of work of the agencies that involve gathering information about individuals and organisations that may intrude into the privacy of individuals and other areas where ministerial guidance was considered appropriate. There are currently 11 MPSs, covering the following activities:
1. Providing information assurance and cybersecurity activities;
  2. Acquiring, using and maintaining an assumed identity;
  3. Creating and maintaining a legal entity (such as a cover company);
  4. Collecting information lawfully from persons without an intelligence warrant (human intelligence activities);
  5. Conducting surveillance in a public place;
  6. Obtaining and using publicly available information (open source information);
  7. Making requests for information from other agencies;
  8. Information management;
  9. Making false or misleading representations about being employed by an intelligence and security agency;
  10. Activities covered by the exemption from the Land Transport (Road User) Rule 2004; and
  11. Cooperation with overseas public authorities, including providing advice and assistance to and sharing intelligence with overseas public authorities.

[HYPERLINK TO EACH]

11. MPSs take effect from the date of signing and continue in effect for three years. The Minister responsible for GCSB and NZSIS may, amend, revoke or replace any of the MPSs at any time. However, they must consult with the Inspector-General of Intelligence and Security, any other relevant Minister, or any other person the Minister considers appropriate.
12. The Minister can issue further MPSs on other areas if considered necessary or desirable.

UNCLASSIFIED



## *Ministerial Policy Statement*

# Cooperating with overseas public authorities

[[Link to landing page on purpose of MPSs](#)]

### Summary

It is important for New Zealand's security for GCSB and NZSIS to cooperate with overseas public authorities, including overseas intelligence agencies.

This Ministerial Policy Statement (MPS) provides guidance for GCSB and NZSIS in relation to cooperation with overseas public authorities. In making decisions related to foreign cooperation, employees must have regard to the following principles: respect for human rights, necessity, reasonableness and proportionality, protections for New Zealanders, information management and oversight. This MPS also specifies additional matters to be included in internal policy and procedures.

### Definitions

**Cooperation** means to work together, and includes sharing intelligence and providing/receiving services, advice or assistance (including training, methodology and technology). This may be reciprocated or unreciprocated.

**Overseas public authority** means a foreign person or body that performs or exercises any public function, duty, or power conferred on that person or body by or under law.

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

### This MPS provides guidance on overseas cooperation

1. New Zealand has a robust legislative framework to govern the activities of GCSB and NZSIS, including activities that involve cooperation with overseas public authorities. The Act includes obligations for GCSB and NZSIS to act in accordance with New Zealand law and all human rights obligations recognised by New Zealand law,<sup>1</sup> independently and impartially, with integrity and professionalism and in a manner that facilitates effective oversight.
2. Cooperation with foreign partners can sometimes pose a risk of acting unlawfully with both domestic legal obligations and international obligations, including a risk that New Zealand could

---

<sup>1</sup> Sections 10(3), 12(7), 17(a) and 18(b).

## UNCLASSIFIED

become complicit in some forms of unlawful conduct by another country.<sup>2</sup> When undertaking overseas cooperation there is also a range of policy, human rights and reputational risks which need to be considered and managed. Consistent with New Zealand's respect for, and promotion of human rights, this MPS therefore provides policy guidance to, and sets expectations on, GCSB and NZSIS that extend beyond their legal obligations.

### Scope of this MPS

3. This MPS applies to GCSB and NZSIS when cooperating with an overseas public authority (whether individually, jointly or with other government agencies). Cooperation may occur in relation to the performance of any of the functions of GCSB and NZSIS in sections 10 to 15 of the Act.
4. Cooperation must be lawful to be within scope of this MPS. Before and during foreign cooperation, GCSB and NZSIS must ensure their actions are consistent with their legal obligations. If in doubt, legal advice must be sought. Failure to act in accordance with New Zealand law could lead to possible criminal responsibility for employees of GCSB and NZSIS.

### Context

#### *Ministerial authorisation to cooperate*

---

5. GCSB and NZSIS must obtain Ministerial authorisation where foreign cooperation involves the provision of intelligence, analysis or threat reporting.<sup>3</sup> Ministerial authorisation can be sought on a case-by-case basis, for example to provide specific intelligence during a conference or event (such as APEC). Alternatively, Ministerial authorisation can be sought on a standing basis to provide intelligence to a range of overseas public authorities on an on-going basis.
6. Standing authorisations must be reviewed regularly to ensure that cooperation undertaken under the authorisation remains consistent with the principles in this MPS. In particular, if there are increased risks for ongoing cooperation either from changes to the domestic law, policy or practice of the overseas public authority subject to a standing authorisation, or from evidence they have carried out a significant breach of human rights, the standing authorisation must be reviewed by the responsible Minister on advice by GCSB and NZSIS.
7. GCSB and NZSIS must ensure sufficient information regarding the human rights practices of the overseas public authority is provided to the Minister to support decision-making. Guidance on this is contained within Appendix One.

#### *New Zealand's intelligence and security relationships*

8. New Zealand gains significant value from cooperating with overseas public authorities, particularly within the current climate of global and transnational threats. Close and reliable intelligence relationships help GCSB and NZSIS prioritise and focus their resources on the areas most important

---

<sup>2</sup> Complicity is a legal term which recognises that while a state did not carry out the wrongful act, if it knowingly aided or assisted another state to commit that wrongful act, it may be liable by law.

<sup>3</sup>By contrast, GCSB and NZSIS may provide protective security services to any public authority in New Zealand or overseas without requiring Ministerial authorisation (in accordance with section 11(1)(a) of the Act).

## UNCLASSIFIED

to New Zealand, while having access to a much greater pool of information, skills and technology that would not otherwise be available to New Zealand.

9. For example, an overseas partner may have specific linguistic or technical capabilities that GCSB and NZSIS need in order to obtain or assess intelligence relevant to New Zealand's security and intelligence priorities. Similarly, GCSB or NZSIS may provide intelligence to an overseas public authority to alert them to a potential threat to their security, which helps contribute to international security and New Zealand's overall international relations with that country.
10. In the context of protective security services, advice and assistance, GCSB or NZSIS may provide technology or expertise to an overseas public authority to develop, implement or improve upon their protective security arrangements - for example, providing expertise on conducting a security vetting assessment, information security systems or detecting and protecting against cybersecurity threats. Such cooperation helps overseas authorities store and protect New Zealand Government information and contributes to the recipient's national security and the security of their region.
11. The closest relationships GCSB and NZSIS have with overseas public authorities are those with equivalent agencies from Australia, Canada, the United Kingdom and the United States (often referred to as the "Five Eyes" partners). The relationships between Five Eyes partners are long-running, reciprocal, cover a wide range of topics, and involve a high degree of mutual trust, honesty and respect. The relationships provide New Zealand with knowledge and capability far beyond what we can afford on our own. These relationships work effectively due to the shared values and histories of the five countries and the strong relations between the governments of those countries. The depth of the Five Eyes relationship means that disparities in size, power and influence do not prevent any member from acting in the best interests of their own government, and members expect to be able to disagree on specific matters without damaging the broader relationship.
12. The GCSB and NZSIS may cooperate with overseas public authorities from countries beyond the Five Eyes. This cooperation may occur on an ongoing, relatively informal, or one-off basis. The reasons for cooperating with such authorities vary widely and may occur while performing any of the agencies' functions and as part of contributing to their objectives. Examples include providing support to a major event such as APEC or the Olympic Games, or helping implement a Protective Security framework with an overseas public authority.

### ***International and domestic obligations***

13. New Zealand's core human rights obligations are detailed at Appendix Two. These include the right to life, the right not to be subjected to torture, the right not to be subjected to cruel, inhuman or degrading treatment or punishment, and the right to liberty and security of the person. New Zealand is also subject to other international obligations. These can be from a range of sources, including customary law obligations or binding United Nations resolutions. These obligations can range in nature from requiring action, prohibiting conduct or recognising rights.
14. The New Zealand Government has a long-standing and strong opposition to the use of torture, cruel, inhuman or degrading treatment or punishment in all cases and under all circumstances, including in response to threats to national security. The prohibition of torture is non-derogable – it can never be violated by states under any circumstances. New Zealand is opposed to the use of



## 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:

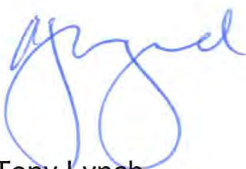
- False or misleading representations about employment;
- Legal entities; and
- Assumed identities.

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

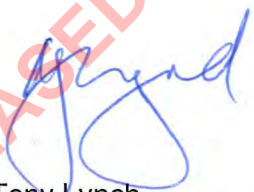
### Purpose

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

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 minor changes to the MPS: Information assurance and cybersecurity activities;
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 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

# 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 <b>Deputy Chief Executive National Security Group</b>
27, 10 ...../...../2021

Hon Andrew Little <b>Minister Responsible for the GCSB Minister Responsible for the NZSIS</b>
...../...../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.

Attachments:		
<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**

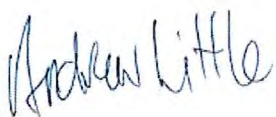
33. Human intelligence activities should be authorised at a level of seniority within GCSB and NZSIS that is commensurate with the level of operational, reputational and legal risk involved. The level of authorisation required should be dictated by the nature of the activity and the assessed overall 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 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**

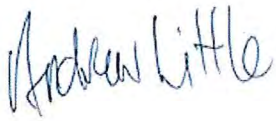
37. GCSB and NZSIS must ensure that where any difficult or sensitive issues regarding the legality or propriety of the collection and use of publicly available information arise, these are dealt with at a sufficiently senior level within the agency. For example, publicly available information may include 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**

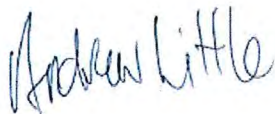
37. The Directors-General of GCSB and NZSIS may delegate their ability to make requests for information consistently with the Public Service Act 2020.
38. All requests for information must be authorised by an appropriately senior employee of the agencies, having regard to the nature of the information 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).